

TRM 2.0  
JUDICIARY  
STANDARDS  
FOR  
INFORMATION  
RESOURCES  
MANAGEMENT



ARCHITECTURE SERIES  
Technical Reference  
Model

Version 2.0  
March 2007

**EXECUTIVE SUMMARY**

# Introduction

The Technical Reference Model (TRM) is part of the Information Systems Architecture (ISA), Information Resources Management Standard (IRMS) 701.1, which is part of the Judicial Enterprise Architecture (JEA).

The ISA is composed two sections: a section that deals with the management and update of the ISA; and the TRM that contains the inventory of standards, guidelines, design principles and products that have been accepted by the ISA.

## The TRM

The Administrative Office (AO) of the U.S. Courts has established an infrastructure for the automation program, including adopting a Technical Reference Model that specifies what kinds of standards, software, and hardware the Judiciary uses to build and operate its application systems.

The purpose of the TRM is to describe the standards and preferred products which form the basis for standardizing the Judiciary's information systems and for evaluating the architecture of proposed new judiciary information systems. The TRM specifies the technical infrastructure (computing and telecommunications standards, hardware, and software), and the principles and standards by which data are to be managed and shared and applications are to be developed. The goal of the TRM is to enable the ability of applications operating on the same or different platforms to communicate, exchange data, share common databases, or share a common service function without significant modification. The TRM is designed to ensure that the Judiciary's expenditures for automated systems are efficiently and wisely made, that user needs are met, and that data and processes can be shared.

The TRM will be used to evaluate any proposal involving information technology (IT) components and to direct the design, construction, deployment, and management of the technology aspects of those projects. The TRM is intended to help programs and projects work within a consistent technology framework throughout the Judiciary.

The TRM is not intended to limit the creativity of projects, but rather to make the outcomes more beneficial and manageable by adhering to architectural principles and IT best practices so that the many interrelated components of such complex systems are highly compatible and work together efficiently. This will ensure that the inventory of hardware, software, and skills can be used to the maximum benefit of the Judiciary.

## The ISA and the TRM

At its June 1996 meeting, the Judicial Conference of the United States' Committee on Automation and Technology (now the Committee on Information Technology) approved the Information Systems Architecture (ISA). At the Committee's recommendation, the Judicial Conference subsequently adopted a policy that all national or multi-circuit IT projects must conform to the ISA, adhere to the IT project management process, and use the IT infrastructure specified within the ISA. The ISA establishes the framework of IT standards, guidelines, and design principles and specifies communications and processing hardware and software that are required to support the business needs and user requirements as described in the *Long Range Plan for Information Technology in the Federal Judiciary*. The goal of the ISA is to promote the seamless sharing of information and judiciary resources in the most cost-effective and flexible manner. The ISA has been incorporated into the IT project management process as Information Resources Management Standard (IRMS) 701.1 (Information Systems Architecture Guidance). Projects expending funds via the Judiciary IT Fund are required to conform to the ISA. The IRMS 301.2 (Project Manager's Handbook) defines the points in the project life cycle that ISA conformance is verified.

The ISA is divided into two parts: the ISA proper, which defines the architecture management and change process; and a separate Technical Reference Model (TRM) which contains the technical core requirements of the ISA. The ISA defines how the TRM is managed and how it is changed to respond to new business requirements. The idea is to separate the process from the product, with an assumption that the TRM may need to be updated frequently, but the process for making those updates will likely not change.

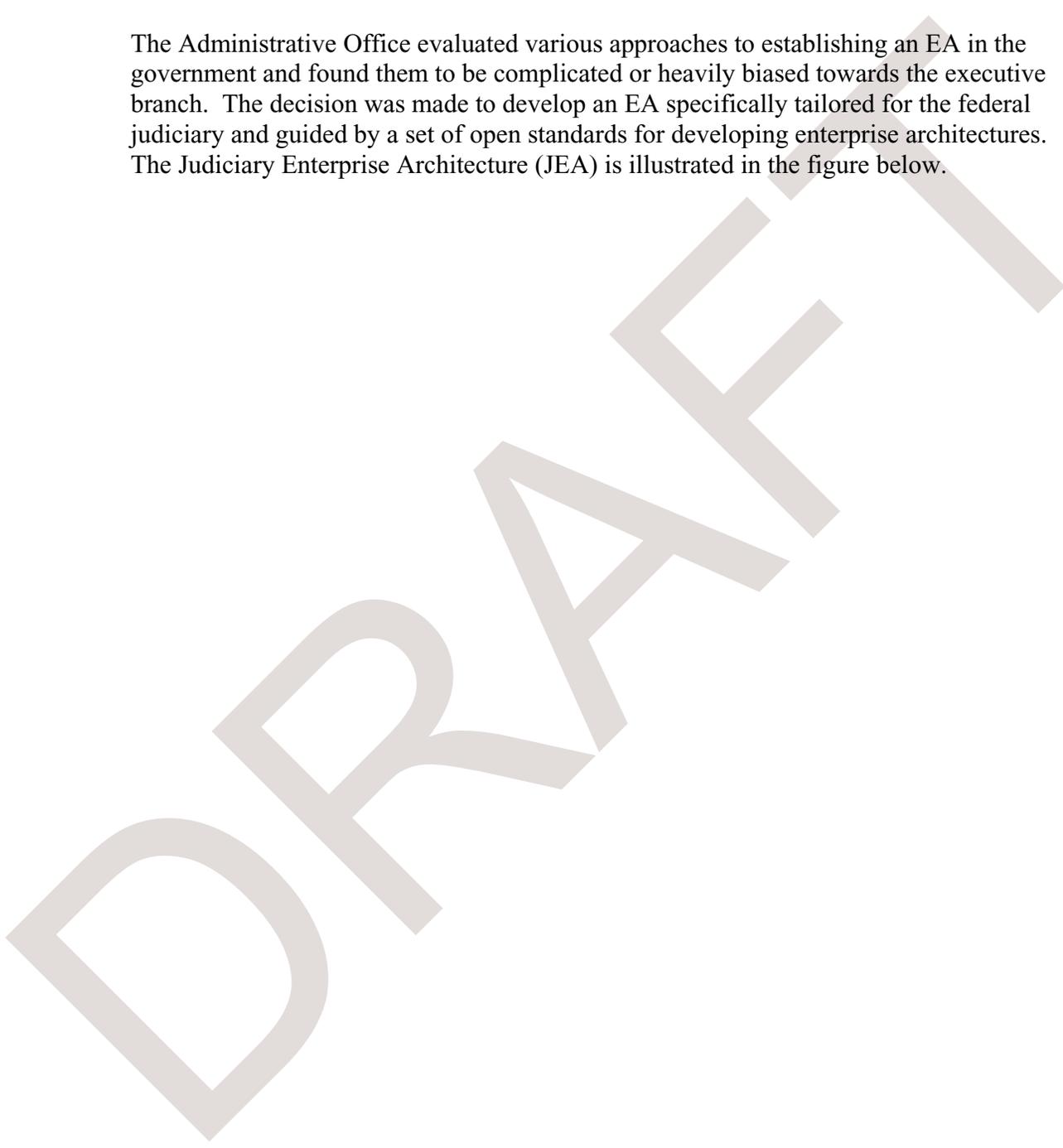
The TRM change process encourages active involvement from the court community, including participation on technology advisory panels to evaluate the impact of new technologies and to recommend appropriate changes to the TRM. Proposed changes to the TRM will be posted for judiciary-wide comment through the "exposure draft" process. The IT Committee will receive periodic notification of technical changes to the TRM product made in accordance with the established ISA management process and it will be asked to concur in any proposed changes to the TRM that would have significant impact on projects, funding, or court operations.

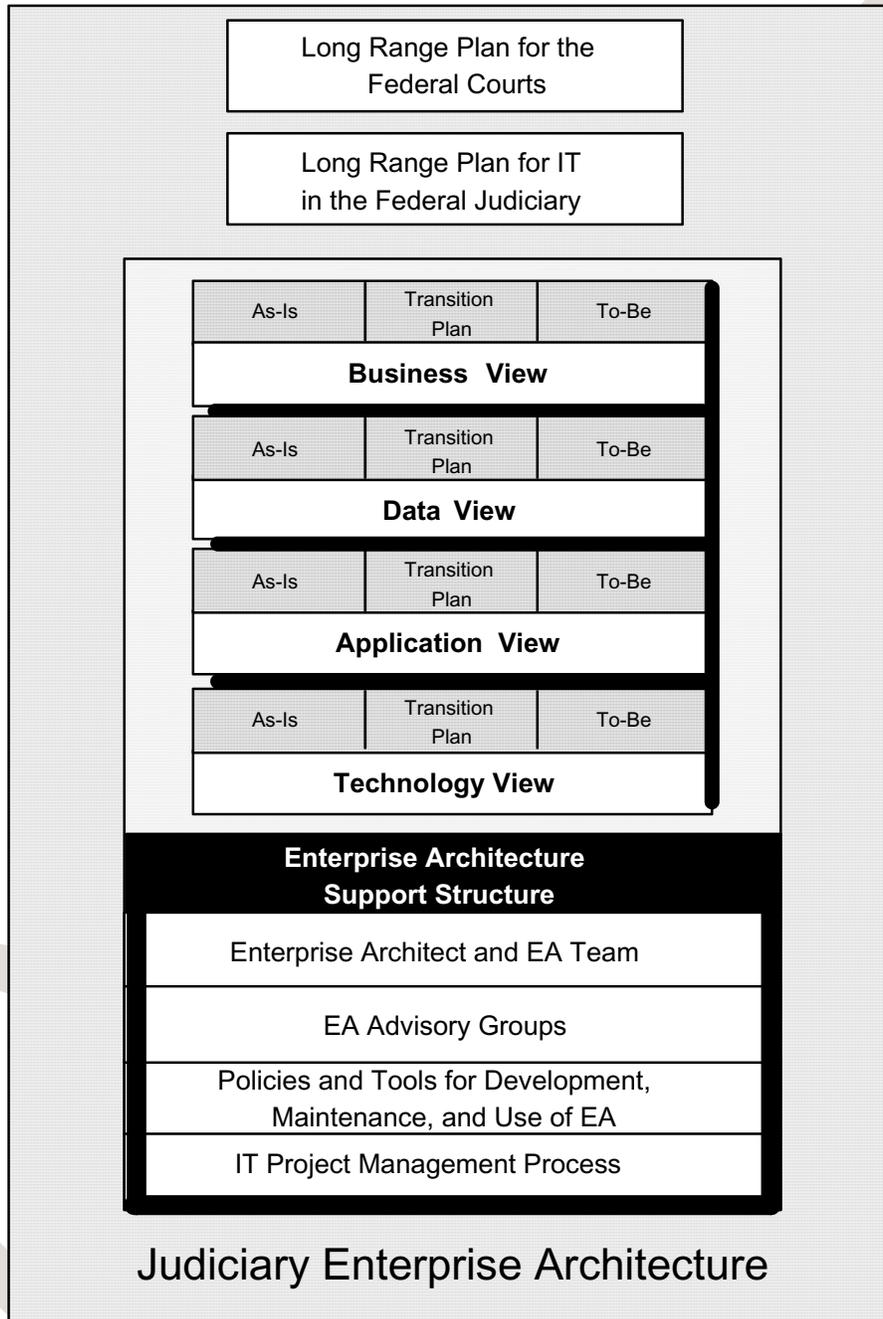
## Judiciary Enterprise Architecture

As noted in the independent study of the Judiciary's IT program conducted by EDS (October 2000), a well-defined enterprise IT architecture is key to creating a judiciary-wide strategy that can maximize the potential benefits of IT investments. This is especially true with the decentralization of business and IT development into separate offices in the AO, and the relative autonomy of the Judiciary's court units in general. An Enterprise Architecture (EA) is a mechanism to ensure the coordination of IT activities across these separate entities. A successful EA will result in more cost-effective IT

systems being implemented. An EA that is integrated with key IT management activities and processes will enable the Judiciary to ensure that its scarce IT resources are spent wisely and that the various IT project managers share a common vision of the judiciary's IT future.

The Administrative Office evaluated various approaches to establishing an EA in the government and found them to be complicated or heavily biased towards the executive branch. The decision was made to develop an EA specifically tailored for the federal judiciary and guided by a set of open standards for developing enterprise architectures. The Judiciary Enterprise Architecture (JEA) is illustrated in the figure below.





**Figure Introduction-1: Judiciary Enterprise Architecture**

The JEA differs from other IT management and EA schemes in that:

- The JEA is fundamentally an IT change management system. The general flow and shape of the desired business changes to be implemented are specified by the *Long Range Plan for the Federal Courts* (December 1995) and the *Long Range Plan for Information Technology in the Federal Judiciary*.
- An Enterprise Architecture deals with an entire business enterprise. In the context of the Judiciary, the scope of the JEA includes any judiciary process that, if automated, uses the Judiciary IT Fund to fund the project.
- The JEA includes (and in fact, starts with) a description of the business of the enterprise within the scope of the JEA. The business of the enterprise drives the JEA. The JEA is intended to be used by both business and IT managers. Business managers use the JEA to facilitate business planning (e.g., to identify business processes that can benefit from the introduction of IT); IT managers use the JEA to guide the effective implementation of IT solutions to meet identified business needs.
- The JEA is layered into views. Each view has a description of the current state of the view (the “As-Is” state), the desired future state of the view (the “To-Be” state), and a transition plan to get from the current state to the future.
- The judiciary JEA has four views: Business, Data, Application, and Technology. The Business View describes the business processes of the enterprise; the Data View describes the data flows supporting the business processes; the Application View describes the software applications supporting the business processes; and the Technology View describes the technical infrastructure used to implement the software applications and data flows supporting the business processes.
- Another name for the Technology View is the Information Systems Architecture (ISA).
- The interrelationships between the various components of each view are also described within the JEA. The Business View is the controlling view—from it the rest of the Enterprise Architecture is derived. The JEA is designed to encourage the goal that IT supports the business of the Judiciary.
- The actual components of the JEA are documents that are maintained by a JEA support database tool. The use of an EA support tool facilitates the use of the JEA and its maintenance.
- Along with the views is a JEA Support Structure that initially creates the JEA and then maintains and facilitates the use of the JEA.
- Key components of the JEA Support Structure are the advisory groups, made up of both business and IT managers and staff drawn from the AO and court units. While the Enterprise Architect and the EA Team are responsible for maintaining the JEA as a resource for decision-making, the advisory groups are responsible for ensuring that the JEA reflects the business needs (As-Is and To-Be) of the Judiciary.
- The enforcement of the JEA is accomplished through the IT Project Management Process.

While filling in the full details necessary to complete the enterprise descriptions for every view is a daunting (and, because of change, perhaps endless) task, it is not necessary to provide the complete details supporting all views of every business process in order to achieve a useful JEA. For example, the Technology View (the ISA/TRM) alone is useful and will benefit the Judiciary.

## TABLE OF CONTENTS

Chapter 1 Introduction .....	1-1
1.1 Overview .....	1-1
1.2 Purpose .....	1-1
1.3 Scope .....	1-1
1.4 Authority .....	1-2
1.5 Responsibility .....	1-2
1.5.1 Assistant Director, Office of Information Technology .....	1-2
1.5.2 OIT - Chief Technology Officer (CTO) .....	1-2
1.5.3 Project Manager .....	1-2
1.5.4 Development Manager .....	1-2
1.6 Intended Audience .....	1-2
1.7 References .....	1-3
1.8 Goals .....	1-4
1.9 Approach .....	1-5
1.10 Definition of Terms .....	1-6
1.11 Document Organization .....	1-6
Chapter 2 Model Components .....	2-1
2.1 Basic Components .....	2-1
2.1.1 Principles .....	2-3
2.2 Component Descriptions .....	2-4
2.2.1 Entities .....	2-4
2.2.1.1 Application Software Entity .....	2-4
2.2.1.2 Application Platform Entity .....	2-4
2.2.1.3 External Environment .....	2-8
2.2.2 Interfaces .....	2-8
2.2.2.1 Application Program Interface (API) .....	2-8
2.2.2.2 External Environment Interface (EEI) .....	2-8
2.3 Detailed Diagram of Model Components .....	2-9
Chapter 3 Application Software Entity .....	3-1
3.1 Overview .....	3-1
3.2 National Applications .....	3-1
3.2.1 CM/ECF .....	3-2
3.2.2 FAS4T and CJA .....	3-2
3.2.3 HRMIS .....	3-2
3.2.4 ILS .....	3-2
3.2.5 JMS .....	3-2
3.2.6 PACER .....	3-2
3.2.7 PACTS .....	3-2
3.2.8 CHASER .....	3-3
3.2.9 CJA .....	3-3
3.2.10 CAS .....	3-3
3.2.11 CVB .....	3-3
3.2.12 NewFACTS .....	3-3
3.2.13 MJSTAR .....	3-3

3.2.14 VCIS .....	3-4
3.2.15 BNC .....	3-4
3.3 Supporting Applications .....	3-4
3.3.1 Electronic Mail Applications .....	3-4
3.3.2 Office Applications.....	3-4
3.4 Local Applications.....	3-4
3.4.1 Executive Support Systems .....	3-5
3.4.1.1 Correspondence Control Management System (CCM) .....	3-5
3.4.1.2 OnTime .....	3-5
3.4.1.3 Major Initiatives Project or Study System (MIPS).....	3-5
3.4.1.4 Judiciary Executive Management System (JEMS).....	3-5
3.4.1.5 Personnel Activities Tracking System (PATS).....	3-6
3.4.2 Financial Information Systems .....	3-6
3.4.2.1 Integrated Court Information System (ICIS) .....	3-6
3.4.2.2 Quarterly Review Application .....	3-6
3.4.2.3 Architectural Statements of Qualifications (AESOP).....	3-7
3.4.2.4 Automated Form AO-15 Requisition.....	3-7
3.4.2.5 Garnishment Information System (Garnisys).....	3-7
3.4.3 Information Dissemination Systems.....	3-7
3.4.3.1 E-Mail Broadcaster .....	3-8
3.4.3.2 Online Legal Information Environment (OLLIE) .....	3-8
3.4.3.3 PeopleFinder .....	3-8
3.4.3.4 Records Management Tracking System (RMTS).....	3-8
3.4.3.5 Guide Enhancement Project.....	3-9
3.4.4 Office Automation Services .....	3-9
3.4.4.1 Electronic Mail Services .....	3-9
3.4.4.2 Enterprise Facsimile Transmission Services .....	3-9
3.4.4.3 Enterprise Print Services.....	3-9
3.4.4.4 Enterprise-Wide Login Services.....	3-10
Chapter 4 Application Platform Entity .....	4-1
4.1 Overview.....	4-1
4.2 Server Hardware .....	4-4
4.3 Operating System (OS) Services .....	4-4
4.3.1 Kernel Operations API .....	4-4
4.3.2 Operating System Commands and Utilities.....	4-5
4.3.3 Operating System Management.....	4-6
4.3.4 Operating System Security .....	4-7
4.4 Software Engineering Services.....	4-8
4.4.1 Overview.....	4-8
4.4.2 System Development Methodology .....	4-9
4.4.3 Business Process Re-engineering .....	4-9
4.4.4 Data Modeling .....	4-10
4.4.5 System Development Tools.....	4-13
4.4.5.1 Primary System Development Tools .....	4-13
4.4.5.2 Web Application Development.....	4-14
4.4.5.3 Web Authoring Tools .....	4-16

4.4.5.4 Traditional Programming Languages .....	4-17
4.4.5.5 Web Application Development Language.....	4-18
4.4.5.6 Web Application Development Environment.....	4-19
4.4.6 System Development Life Cycle .....	4-19
4.4.6.1 Project Management .....	4-20
4.4.6.2 Requirements Management .....	4-20
4.4.6.3 Configuration Management .....	4-21
4.4.6.4 Test Management.....	4-22
4.5 Human Computer Interface Services.....	4-23
4.5.1 Traditional Graphical User Interface.....	4-23
4.5.2 Web Graphical User Interface .....	4-24
4.5.2.1 Web Browser .....	4-25
4.5.2.2 Web Server.....	4-26
4.5.3 Alternate User Interface.....	4-27
4.5.4 Multimedia Interface .....	4-29
4.5.5 Terminal Emulation .....	4-30
4.6 Data Management Services.....	4-31
4.6.1 Metadata Repository .....	4-32
4.6.2 Metadirectory Services .....	4-33
4.6.3 Online Analytical Processing (OLAP) .....	4-34
4.6.3.1 (OLAP) Servers .....	4-35
4.6.3.2 Desktop and Online Analytical Processing (OLAP / DOLAP).....	4-36
4.6.4 Data Extraction, Transformation, and Load (ETL) Tools .....	4-36
4.6.5 Search Services.....	4-37
4.6.6 Document Management.....	4-37
4.6.7 Electronic Records Management.....	4-38
4.6.8 Web Content Management (WCM).....	4-39
4.6.9 Image and Multimedia Management Systems.....	4-41
4.6.10 Database Management Systems (DBMS) .....	4-42
4.6.11 Database Environments .....	4-44
4.6.12 Data Management Security.....	4-45
4.7 Data Interchange Services.....	4-47
4.7.1 Financial and Human Resources Technical Standards.....	4-47
4.7.2 Library Interchange Standards.....	4-48
4.7.3 Unicode Standard.....	4-49
4.7.4 Markup Languages .....	4-50
4.7.4.1 Standard Generalized Markup Language.....	4-50
4.7.4.2 Extensible Markup Language ).....	4-51
4.7.4.3 Hypertext Markup Language .....	4-51
4.7.4.4 Extensible Hypertext Markup Language .....	4-52
4.7.4.5 Cascading Style Sheets .....	4-52
4.7.4.6 Extensible Stylesheet Language .....	4-52
4.7.5 Portable Document Format.....	4-54
4.7.6 File Compression Formats.....	4-55
4.7.7 Office Automation File Formats.....	4-56
4.7.8 Calendar Date and Ordinal Date Interchange Format .....	4-58

4.7.9 Vector Graphics .....	4-58
4.7.10 Raster Image Interchange Format.....	4-59
4.7.11 Tagged Image File Format.....	4-59
4.7.12 Joint Photographic Experts Group.....	4-60
4.7.13 Motion Picture Experts Group.....	4-61
4.7.14 Electronic Data Interchange .....	4-63
4.7.15 Computer-Aided Design Data .....	4-63
4.8 Graphics Services.....	4-64
4.9 Computer-Based Interactive Training.....	4-65
4.10 Output Services.....	4-66
4.10.1 Facsimile Transmission Service (fax) .....	4-66
4.10.2 Compact Disk-Read Only (CD-ROM) Generation Service .....	4-66
4.10.3 Digital Versatile Disc (DVD) ) Generation Service .....	4-67
4.10.4 Digital Video and Film Generation Service .....	4-68
4.10.5 Magnetic Tape Generation Service .....	4-68
4.10.6 Plotting Service.....	4-70
4.10.7 Print Service.....	4-70
4.11 Network Services.....	4-71
4.11.1 National Internet Gateways .....	4-73
4.11.2 DCN/Backbone Configuration .....	4-74
4.11.3 PacerNet.....	4-76
4.11.4 Network File and Print Services.....	4-77
4.11.5 Directory and Naming Services.....	4-79
4.11.6 Domain Name Service.....	4-81
4.11.7 Electronic Mail and Message Services.....	4-82
4.11.8 Time Services .....	4-84
4.12 Videoconferencing.....	4-85
4.13 Virtual LAN.....	4-86
4.14 Voice Over IP (VoIP) .....	4-87
4.15 Communication Protocols.....	4-88
4.15.1 Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).....	4-88
4.15.2 Transmission Control Protocol / Internet Protocol (TCP/IP) .....	4-89
4.15.2.1 Internet Control Message Protocol (ICMP).....	4-92
4.15.2.2 Address Resolution Protocol (ARP).....	4-92
4.15.2.3 Routing Protocols.....	4-92
4.15.3 Ethernet.....	4-93
4.15.3.1 Gigabit Ethernet.....	4-94
4.15.4 Wireless Local Area Network .....	4-95
4.15.5 Frame Relay.....	4-97
4.15.6 Asynchronous Transfer Mode .....	4-97
4.15.6.1 LAN Emulation.....	4-100
4.15.6.2 Emulated LAN.....	4-100
4.15.6.3 Multi-Protocol Over ATM.....	4-101
4.15.7 Dynamic Host Configuration Protocol .....	4-101
4.15.8 Hypertext Transfer Protocol .....	4-103
4.15.9 Uniform Resource Locator .....	4-104

4.15.10 Multipurpose Internet Mail Extensions)	4-105
4.16 Security Services	4-106
4.16.1 Network Security Services	4-106
4.16.1.1 Secure Firewall	4-107
4.16.1.2 Intrusion Detection	4-108
4.16.2 Authentication	4-111
4.16.2.1 Authentication Protocols/Password Authentication Protocol	4-112
4.16.2.2 Access Authentication Protocols	4-113
4.16.3 Access Control	4-114
4.16.3.1 Password Usage	4-115
4.16.4 Confidentiality, Integrity, and Non-Repudiation	4-115
4.16.4.1 Encryption/Cryptography	4-116
4.16.4.1.1 Symmetric-key or Private-key Cryptography	4-116
4.16.4.1.2 Public-Key or Asymmetric Cryptography	4-116
4.16.4.1.3 Data Encryption Standard	4-117
4.16.4.1.4 Triple-DES (3DES)	4-118
4.16.4.2 Electronic Commerce Security Services	4-118
4.16.4.3 Virtual Private Network	4-119
4.16.4.4 Virus Control	4-121
4.16.4.5 Public Key Infrastructure	4-122
4.16.4.5.1 Digital Signature Standard	4-122
4.16.4.5.2 Digital Certificate Authentication (X.509)	4-123
4.16.4.5.3 Digital Time Stamp	4-123
4.16.4.5.4 Secure Hash Standard	4-123
4.16.4.6 Security Protocols	4-124
4.16.4.6.1 Transport Layer Security	4-124
4.16.4.6.2 Secure Sockets Layer	4-125
4.16.4.6.3 Secure Multipurpose Internet Mail Extensions (S/MIME)	4-125
4.16.4.6.4 Message-Digest Algorithms	4-126
4.16.4.6.5 Audit	4-126
4.16.4.7 Access Filtering, Monitoring, and Reporting	4-127
4.16.5 Security Administration	4-127
4.17 System and Network Management Services	4-127
4.17.1 Network System Administration	4-128
4.17.2 Help Desk Administration	4-129
4.17.3 Communication Network Management	4-130
4.17.4 Server Management	4-132
4.17.5 Capacity Planning and Performance Management	4-132
4.17.6 Backup and Recovery Service	4-133
4.18 Distributed Computing Services	4-134
4.18.1 Distributed Computing Application Services	4-135
4.18.2 Three-Tier Web-enabled DCA Model	4-136
4.18.3 Distributed Computing Architecture Framework	4-139
4.18.4 Internet/Extranet Architecture Option	4-142
4.18.5 Intranet Architecture Option	4-143
4.18.6 Overview of DCAF Standards and Functional Elements	4-143

4.18.7 Online Transaction Processing .....	4-146
4.18.8 Distributed Computing Application Security .....	4-147
4.18.9 Message Queuing.....	4-148
4.18.10 Web Services .....	4-148
Chapter 5 External Environment .....	5-1
5.1 Introduction.....	5-1
5.2 User Desktop Workstations .....	5-2
5.3 Information Exchange Media .....	5-2
5.3.1 Media .....	5-2
5.3.2 Tape .....	5-6
5.3.3 CD-ROM Server and Magnetic Optical Disk.....	5-7
5.3.4 Digital Versatile Disc) Generation Service .....	5-8
5.3.5 Scanners.....	5-8
5.4 Output Devices.....	5-9
5.4.1 Displays .....	5-9
5.4.1.1 Direct View Monitors .....	5-9
5.4.1.2 Array of Monitors .....	5-10
5.4.1.3 Front Projection .....	5-10
5.4.1.4 Rear Projection.....	5-10
5.4.2 Printers.....	5-10
5.5 Information Storage .....	5-11
5.5.1 Magnetic Disk Storage .....	5-11
5.5.2 Server Attached Local Disk Array .....	5-12
5.5.3 Network Attached Storage.....	5-12
5.5.4 Storage Area Networks.....	5-13
5.6 Communications Hardware .....	5-14
5.6.1 Cables .....	5-14
5.6.2 Bridges, Routers, and Switches .....	5-15
5.7 Satellite Broadcasting/FJTN .....	5-16
Chapter 6 Judiciary Current and Target Architecture.....	6-1
6.1 TRM in the Context of the Federal Enterprise Architecture Framework .....	6-1
6.2 Judiciary Profiles of Standards .....	6-2
6.2.1 Open Systems Standards.....	6-2
6.2.2 Profile of Standards .....	6-3
APPENDIX A ACCESS TO THE TRM.....	A-2
A.1 Access to the TRM.....	A-2
A.2 Points of Contact.....	A-2
A.3 TRM Update Process - Role of TWGs in Recommending a Preferred Product.....	A-2
APPENDIX B Standards Profile.....	B-1
APPENDIX C Judiciary Profile of Preferred Products.....	C-1
C.1 CHAPTER 4- APPLICATION PLATFORM ENTITY .....	C-1
APPENDIX D SDSD RAID Standards.....	D-1
D.1 RAID Standards.....	D-1
D.2 Disk Configuration Standards.....	D-1
D.2.1 Physical Disk Placement.....	D-1
D.2.1.1 Root Storage Array .....	D-1

D.2.1.2	Application Server Storage Array.....	D-1
D.3	RAID 5.....	D-2
D.3.1	Minimum and Maximum Disks.....	D-2
D.3.2	Hot Spare .....	D-2
D.3.3	Location .....	D-3
D.4	Data Configuration Standards.....	D-3
D.4.1	Data Placement .....	D-3
D.4.1.1	Root Disk .....	D-3
D.4.1.2	/usr.....	D-3
D.4.1.3	/gov .....	D-3
D.4.1.4	Packaging.....	D-4
D.4.2	Software Standards .....	D-4
D.4.2.1	Application Logs.....	D-4
D.4.2.2	Start/Stop Scripts .....	D-4
D.4.2.3	Path Names .....	D-4
D.4.2.4	Symbolic Links .....	D-4
D.4.2.5	Local Applications.....	D-4
D.5	Server Configuration Standards.....	D-5
D.5.1	CM/ECF Outside Server.....	D-5
D.5.1.1	9.1-GB Disks.....	D-5
D.5.1.2	18-GB Disks.....	D-5
D.5.2	Application Server Storage Array(s) .....	D-5
D.5.2.1	Root Storage.....	D-6
D.5.2.2	9.1-GB Disks.....	D-6
D.5.2.3	18-GB disks .....	D-6
D.5.3	Application Storage .....	D-6
D.6	Application Storage Directory Standards .....	D-7
D.6.1	Required Directory Structure.....	D-7
D.6.2	JMS /app01 Directory .....	D-9
D.6.3	FAS4T /app01 Directory.....	D-10
D.6.4	CM/ECF /app## Directory.....	D-11
D.6.5	PACTS /app## Directory.....	D-13
APPENDIX E	WORKSTATION CONFIGURATIONS .....	E-1
E.1	Minimum Client Hardware Requirements.....	E-1
E.1.1	Light Client (e.g., browser interface).....	E-1
E.1.2	Medium Client (e.g., browser with active components).....	E-1
E.1.3	Heavy Client (e.g., application on client with network access to database or backend) .....	E-1
APPENDIX F	ACRONYMS.....	F-1
APPENDIX G	REFERENCES .....	G-1

## LIST OF FIGURES

Figure Introduction-1: Judiciary Enterprise Architecture.....	vi
Figure 2.1-1: TRM High-Level Elements.....	2-2
Figure 2.1-2: TRM Basic Components.....	2-4
Figure 2.3-1: Judiciary Technical Reference Model Detail Level.....	2-10
Figure 3.1-1: Diagram of Application Software Entity .....	3-1
Figure 4.1-1: Application Platform Entity Diagram.....	4-3
Figure 4.11-4.11-1: Two National Gateways Service Areas.....	4-73
Figure 4.11-4.11-2: National Gateway for DCN, PacerNet, and Network Services.....	4-75
Figure 4.11-4.11-3: National E-Mail Gateway.....	4-83
Figure 4.15-4.15-1: Mapping of the TCP/IP Suite to the OSI Model.....	4-91
Figure 4.15-4.15-2: ATM Reference Model.....	4-99
Figure 4.16-4.16-1: National Gateway Intrusion Detection System (IDS) .....	4-110
Figure 4.16-4.16-2: Standard US Courts VPN Configuration.....	4-120
Figure 4.18-4.18-1: Physical View of the Generic 3-Tier Web-Enabled DCA Model .....	4-136
Figure 4.18-4.18-2: Current Functional and Physical Mapping.....	4-137
Figure 4.18-4.18-3: J2EE Future Functional and Physical Mapping.....	4-138
Figure 4.18-4.18-4: Distributed Computing Architecture Framework (DCAF).....	4-140
Figure 4.18-4.18-5: DCA Framework with Options.....	4-141
Figure 4.18-4.18-6: Class 1 Option Architecture Framework .....	4-142
Figure 4.18-4.18-7: Class 2 Option Architecture Framework .....	4-143
Figure 4.18-4.18-8: J2EE Container-Based Component Management Model.....	4-145
Figure 4.18-4.18-9: Web Application Server Framework.....	4-145
Figure 4.18-4.18-10: Service-Oriented Architecture (SOA) .....	4-149
Figure 4.18-4.18-11: Web Services Stack .....	4-150
Figure 5.1-1: Judicial External Environment.....	5-1
Figure 6.1-1: Concept of the Federal Enterprise Architecture Framework .....	6-1
Figure 6.1-2: Judiciary Enterprise IT Architecture Strategy .....	6-2
Figure 6.2-1: Judiciary Profile of Standards.....	6-4
Figure 6.2-2: Judiciary Profile of Preferred Products.....	6-5
Figure D-2: Example of Hot Spare Configuration.....	D-3

## LIST OF TABLES

Table 2.2-1: Application Platform Services.....	2-5
Table 4.3-1: Kernel Operations Products Used by the Judiciary.....	4-4
Table 4.3-2: Kernel Operations Preferred Products for the Judiciary .....	4-5
Table 4.3-3: Kernel Operations Proposed Products for the Judiciary .....	4-5
Table 4.3-4: Additional OS Products Used by the Judiciary .....	4-6
Table 4.3-5: OS Preferred Products for the Judiciary.....	4-6
Table 4.3-6: OS Management Products Used by the Judiciary:.....	4-7
Table 4.3-7: OS Management Preferred Products for the Judiciary.....	4-7
Table 4.3-8: OS Management Proposed Products for the Judiciary.....	4-7
Table 4.3-9: OS Security Products Used by the Judiciary.....	4-8

Table 4.3-10: OS Security Preferred Products for the Judiciary: .....	4-8
Table 4.4-1: BPR Products Used by the Judiciary.....	4-10
Table 4.4-2: BPR Preferred Products for the Judiciary .....	4-10
Table 4.4-3: Data Modeling Products Used by the Judiciary .....	4-12
Table 4.4-4: Data Modeling Preferred Products for the Judiciary.....	4-13
Table 4.4-5: System Development Tool Products Used by the Judiciary .....	4-14
Table 4.4-6: System Development Tool Preferred Products for the Judiciary .....	4-14
Table 4.4-7: Web Application Development Products Used by the Judiciary .....	4-15
Table 4.4-8: Web Application Development Preferred Products for the Judiciary.....	4-15
Table 4.4-9: Web Application Development Proposed Products for the Judiciary.....	4-15
Table 4.4-10: Web Authoring Tool Products Used by the Judiciary.....	4-16
Table 4.4-11: Web Authoring Tool Preferred Products for the Judiciary .....	4-17
Table 4.4-12: Programming Language Products Used by the Judiciary .....	4-17
Table 4.4-13: Programming Language Preferred Products for the Judiciary .....	4-17
Table 4.4-14: Web Application Language Products Used by the Judiciary .....	4-18
Table 4.4-15: Web Application Language Preferred Products for the Judiciary.....	4-18
Table 4.4-16: IDE Products Used by the Judiciary.....	4-19
Table 4.4-17: IDE Preferred Products for the Judiciary .....	4-19
Table 4.4-18: PM Products Used by the Judiciary .....	4-20
Table 4.4-19: Preferred Products for the Judiciary.....	4-20
Table 4.4-20: RM Products Used by the Judiciary .....	4-21
Table 4.4-21: RM Preferred Products for the Judiciary.....	4-21
Table 4.4-22: CM Products Used by the Judiciary .....	4-22
Table 4.4-23: CM Preferred Products for the Judiciary.....	4-22
Table 4.4-24: CM Proposed Products for the Judiciary.....	4-22
Table 4.5-1: GUI Products Used by the Judiciary .....	4-24
Table 4.5-2: GUI Preferred Product for the Judiciary .....	4-24
Table 4.5-3: Web Browser Products Used by the Judiciary .....	4-25
Table 4.5-4: Web Browser Preferred Products for the Judiciary.....	4-25
Table 4.5-5: Web Server Products Used by the Judiciary .....	4-27
Table 4.5-6: Web Server Preferred Products for the Judiciary.....	4-27
Table 4.5-7: Alternate User Interface Products Used by the Judiciary.....	4-28
Table 4.5-8: Alternate User Interface Preferred Products for the Judiciary .....	4-29
Table 4.5-9: Alternate User Interface Proposed Products for the Judiciary .....	4-29
Table 4.5-10: Multimedia Interface Products Used by the Judiciary .....	4-30
Table 4.5-11: Multimedia Interface Preferred Products for the Judiciary .....	4-30
Table 4.5-12: Terminal Emulation Products Used by the Judiciary.....	4-30
Table 4.5-13: Terminal Emulation Preferred Products for the Judiciary.....	4-31
Table 4.6-1: Metadata Repository Products Used by the Judiciary.....	4-33
Table 4.6-2: Metadata Repository Preferred Products for the Judiciary .....	4-33
Table 4.6-3: Metadata Repository Proposed Products for the Judiciary .....	4-33
Table 4.6-4: Metadata Repository Products to Which the Judiciary Will Evolve.....	4-33
Table 4.6-5: Metadirectory Service Products Used by the Judiciary.....	4-34
Table 4.6-6: Metadirectory Service Preferred Products for the Judiciary .....	4-34
Table 4.6-7: OLAP Products Used by the Judiciary.....	4-35
Table 4.6-8: OLAP Preferred Products for the Judiciary .....	4-36

Table 4.6-9: OLAP/DOLAP Products Used by the Judiciary .....	4-36
Table 4.6-10: OLAP/DOLAP Preferred Products for the Judiciary .....	4-36
Table 4.6-11: ETL Tool Products Used by the Judiciary .....	4-36
Table 4.6-12: ETL Tool Preferred Products for the Judiciary .....	4-36
Table 4.6-13: Full-Text Search Products Used by the Judiciary .....	4-37
Table 4.6-14: Full-Text Search Preferred Products for the Judiciary .....	4-37
Table 4.6-15: Document Management Products Used by the Judiciary .....	4-38
Table 4.6-16: Document Management Proposed Products for the Judiciary .....	4-38
Table 4.6-17: ERM Products Used by the Judiciary .....	4-39
Table 4.6-18: ERM Preferred Products for the Judiciary .....	4-39
Table 4.6-19: ERM Proposed Products for the Judiciary .....	4-39
Table 4.6-20: Web Content Management Products Used by the Judiciary .....	4-40
Table 4.6-21: Web Content Management Preferred Products for the Judiciary .....	4-40
Table 4.6-22: Web Content Management Proposed Products for the Judiciary .....	4-41
Table 4.6-23: Multimedia Products Used by the Judiciary .....	4-41
Table 4.6-24: Multimedia Preferred Products for the Judiciary .....	4-42
Table 4.6-25: DBMS Products Used by the Judiciary .....	4-43
Table 4.6-26: DBMS Preferred Products for the Judiciary .....	4-43
Table 4.6-27: DBMS Proposed Products for the Judiciary .....	4-43
Table 4.6-28: Database Environment Products Used by the Judiciary .....	4-45
Table 4.6-29: Database Environment Preferred Product for the Judiciary .....	4-45
Table 4.6-30: Data Management Security Products Used by the Judiciary .....	4-46
Table 4.6-31: Data Management Security Preferred Products for the Judiciary .....	4-46
Table 4.7-1: JFMIP Products Used by the Judiciary .....	4-48
Table 4.7-2: JFMIP Preferred Products for the Judiciary .....	4-48
Table 4.7-3: JFMIP Products for the Judiciary .....	4-48
Table 4.7-4: Library Interchange Standards Products Used by the Judiciary .....	4-49
Table 4.7-5: Library Interchange Standards Preferred Products for the Judiciary .....	4-49
Table 4.7-6: Unicode Standard Products Used by the Judiciary .....	4-50
Table 4.7-7: Unicode Standard Preferred Products for the Judiciary .....	4-50
Table 4.7-8: XSL Products Used by the Judiciary .....	4-53
Table 4.7-9: XSL Preferred Products for the Judiciary .....	4-54
Table 4.7-10: PDF Products Used by the Judiciary .....	4-54
Table 4.7-11: PDF Preferred Products for the Judiciary .....	4-55
Table 4.7-12: Compression Formats for the Judiciary .....	4-56
Table 4.7-13: File Compression Products Used by the Judiciary .....	4-56
Table 4.7-14: File Compression Preferred Products for the Judiciary .....	4-56
Table 4.7-15: Office Automation File Format Products Used by the Judiciary .....	4-57
Table 4.7-16: Office Automation File Format Preferred Products for the Judiciary .....	4-57
Table 4.7-17: Office Automation File Format Proposed Products for the Judiciary .....	4-57
Table 4.7-18: Date Interchange Format Products Used by the Judiciary .....	4-58
Table 4.7-19: Date Interchange Preferred Products for the Judiciary .....	4-58
Table 4.7-20: SVG Products Used by the Judiciary .....	4-59
Table 4.7-21: SVG Preferred Products for the Judiciary .....	4-59
Table 4.7-22: Raster Image Interchange Products Used by the Judiciary .....	4-59
Table 4.7-23: Raster Image Interchange Preferred Products for the Judiciary .....	4-59

Table 4.7-24: TIFF Products Used by the Judiciary .....	4-60
Table 4.7-25: TIFF Preferred Products for the Judiciary.....	4-60
Table 4.7-26: JPEG Products Used by the Judiciary .....	4-61
Table 4.7-27: JPEG Preferred Products for the Judiciary.....	4-61
Table 4.7-28: MPEG Products Used by the Judiciary .....	4-62
Table 4.7-29: MPEG Preferred Products for the Judiciary.....	4-62
Table 4.7-30: MPEG Proposed Products for the Judiciary.....	4-62
Table 4.7-31: EDI Products Used by the Judiciary.....	4-63
Table 4.7-32: EDI Preferred Products for the Judiciary .....	4-63
Table 4.7-33: CAD Products Used by the Judiciary.....	4-64
Table 4.7-34: CAD Preferred Products for the Judiciary .....	4-64
Table 4.8-1: Graphics Services Products Used by the Judiciary .....	4-65
Table 4.8-2: Graphics Services Preferred Products for the Judiciary.....	4-65
Table 4.9-1: Computer-Based Interactive Training Products Used by the Judiciary .....	4-65
Table 4.9-2: Computer-Based Interactive Training Preferred Products for the Judiciary .....	4-65
Table 4.9-3: Computer-Based Interactive Training Proposed Products for the Judiciary .....	4-65
Table 4.10-1: Facsimile Products Used by the Judiciary.....	4-66
Table 4.10-2: Facsimile Preferred Products for the Judiciary .....	4-66
Table 4.10-3: Facsimile Proposed Products for the Judiciary .....	4-66
Table 4.10-4: CD-ROM Products Used by the Judiciary .....	4-67
Table 4.10-5: CD-ROM Preferred Products for the Judiciary.....	4-67
Table 4.10-6: DVD Products Used by the Judiciary.....	4-68
Table 4.10-7: DVD Preferred Products for the Judiciary .....	4-68
Table 4.10-8: Digital Video Generation Products Used by the Judiciary.....	4-68
Table 4.10-9: Digital Video Generation Preferred Products for the Judiciary .....	4-68
Table 4.10-10: Magnetic Tape Products Used by the Judiciary .....	4-69
Table 4.10-11: Magnetic Tape Preferred Products for the Judiciary.....	4-69
Table 4.10-12: Magnetic Tape Proposed Products for the Judiciary.....	4-70
Table 4.10-13: Plotting Service Products Used by the Judiciary.....	4-70
Table 4.10-14: Plotting Service Preferred Products for the Judiciary .....	4-70
Table 4.10-15: Print Service Products Used by the Judiciary .....	4-71
Table 4.10-16: Print Service Preferred Products for the Judiciary .....	4-71
Table 4.10-17: Print Service Proposed Products for the Judiciary .....	4-71
Table 4.11-1: National Internet Gateway Products Used by the Judiciary.....	4-73
Table 4.11-2: National Internet Gateway Preferred Product for the Judiciary.....	4-73
Table 4.11-3: DCN Products Used by the Judiciary.....	4-75
Table 4.11-4: DCN Preferred Products for the Judiciary .....	4-75
Table 4.11-5: PacerNet Products Used by the Judiciary.....	4-77
Table 4.11-6: PacerNet Preferred Products for the Judiciary .....	4-77
Table 4.11-7: NOS Products Used by the Judiciary .....	4-78
Table 4.11-8: NOS Preferred Products for the Judiciary .....	4-79
Table 4.11-9: NOS Proposed Products for the Judiciary.....	4-79
Table 4.11-10: Directory Service Products Used by the Judiciary.....	4-81
Table 4.11-11: Directory Service Preferred Products for the Judiciary.....	4-81
Table 4.11-12: Directory Service Proposed Products for the Judiciary.....	4-81
Table 4.11-13: DNS Products Used by the Judiciary .....	4-82

Table 4.11-14: DNS Preferred Products for the Judiciary .....	4-82
Table 4.11-15: E-mail and Messaging Products Used by the Judiciary .....	4-84
Table 4.11-16: E-mail and Messaging Preferred Products for the Judiciary .....	4-84
Table 4.11-17: Time Service Products Used by the Judiciary .....	4-85
Table 4.11-18: Time Service Preferred Products for the Judiciary .....	4-85
Table 4.12-1: Videoconferencing Products Used by the Judiciary.....	4-86
Table 4.12-2: Videoconferencing Preferred Products for the Judiciary .....	4-86
Table 4.13-1: VLAN Products Used by the Judiciary .....	4-87
Table 4.13-2: VLAN Preferred Products for the Judiciary.....	4-87
Table 4.14-1: VoIP Products Used by the Judiciary.....	4-87
Table 4.14-2: VoIP Preferred Product for the Judiciary .....	4-87
Table 4.15-1: IPX/SPX Products Used by the Judiciary .....	4-89
Table 4.15-2: IPX/SPX Preferred Products for Judiciary.....	4-89
Table 4.15-3: TCP/IP Products Used by the Judiciary .....	4-91
Table 4.15-4: TCP/IP Preferred Products for the Judiciary.....	4-92
Table 4.15-5: Ethernet Products Used by the Judiciary.....	4-94
Table 4.15-6: Ethernet Preferred Products for the Judiciary .....	4-94
Table 4.15-7: Gigabit Ethernet Products Used by the Judiciary.....	4-95
Table 4.15-8: Gigabit Ethernet Preferred Products for the Judiciary .....	4-95
Table 4.15-9 <i>WLAN Products Used by the Judiciary</i> .....	4-97
Table 4.15-10: Preferred Products for the Judiciary .....	4-97
Table 4.15-11: Frame Relay Products Used by the Judiciary.....	4-97
Table 4.15-12: Frame Relay Preferred Products for the Judiciary .....	4-97
Table 4.15-13: ATM Products Used by the Judiciary .....	4-99
Table 4.15-14: ATM Preferred Products for the Judiciary .....	4-99
Table 4.15-15: LANE Products Used by the Judiciary.....	4-100
Table 4.15-16: LANE Preferred Products for the Judiciary .....	4-100
Table 4.15-17: ELAN Products Used by the Judiciary.....	4-100
Table 4.15-18: ELAN Preferred Products for the Judiciary .....	4-100
Table 4.15-19: MPOA Products Used by the Judiciary.....	4-101
Table 4.15-20: MPOA Preferred Products for the Judiciary .....	4-101
Table 4.15-21: DHCP Products Used by the Judiciary.....	4-102
Table 4.15-22: DHCP Preferred Products for the Judiciary .....	4-102
Table 4.15-23: MIME Products Used by the Judiciary .....	4-105
Table 4.15-24: MIME Preferred Products for the Judiciary.....	4-105
Table 4.16-1: Security Firewall Products Used by the Judiciary.....	4-108
Table 4.16-2: Security Firewall Preferred Products for the Judiciary .....	4-108
Table 4.16-3: IDS Products Used by the Judiciary.....	4-111
Table 4.16-4: IDS Preferred Products for the Judiciary .....	4-111
Table 4.16-5: Authentication Protocol Products Used by the Judiciary.....	4-113
Table 4.16-6: Authentication Protocol Preferred Products for the Judiciary.....	4-113
Table 4.16-7: Access Authentication Protocol Products Used by the Judiciary.....	4-113
Table 4.16-8: Access Authentication Protocol Preferred Products for the Judiciary .....	4-114
Table 4.16-9: Access Control Products Used by the Judiciary.....	4-114
Table 4.16-10: Access Control Product Preferred Products for the Judiciary.....	4-115
Table 4.16-11: Password Usage Products Used by the Judiciary.....	4-115

Table 4.16-12: Password Usage Preferred Products for the Judiciary.....	4-115
Table 4.16-13: VPN Products Used by the Judiciary .....	4-120
Table 4.16-14: VPN Preferred Products for the Judiciary .....	4-121
Table 4.16-15: Virus Control Products Used by the Judiciary .....	4-121
Table 4.16-16: Virus Control Preferred Products for the Judiciary.....	4-122
Table 4.16-17: X.509 Products Used by the Judiciary .....	4-123
Table 4.16-18: X.509 Preferred Products for the Judiciary .....	4-123
Table 4.17-1: Network System Administration Products Used by the Judiciary .....	4-128
Table 4.17-2: Network System Administration Preferred Products for the Judiciary.....	4-129
Table 4.17-3: Help Desk Products Used by the Judiciary .....	4-129
Table 4.17-4: Preferred Help Desk Products for the Judiciary .....	4-130
Table 4.17-5: Network Management Products Used by the Judiciary .....	4-131
Table 4.17-6: Network Management Preferred Products for the Judiciary .....	4-131
Table 4.17-7: Server Management Products Used by the Judiciary .....	4-132
Table 4.17-8: Server Management Preferred Products for the Judiciary.....	4-132
Table 4.17-9: Capacity Planning/Performance Management Products Used by the Judiciary .....	4-133
Table 4.17-10: Capacity Planning/Performance Management Preferred Products for the Judiciary .....	4-133
Table 4.17-11: Backup Products Used by the Judiciary .....	4-134
Table 4.17-12: Backup Preferred Products for the Judiciary.....	4-134
Table 4.18-1: Generic 3-Tier Distributed Systems Application Model.....	4-135
Table 5.2-1: Desktop Workstation Products Used by the Judiciary .....	5-2
Table 5.2-2: Desktop Workstation Preferred Products for the Judiciary.....	5-2
Table 5.3-1: Tape Products Used by the Judiciary .....	5-7
Table 5.3-2: Tape Product Preferred Products for the Judiciary .....	5-7
Table 5.3-3: Tape Product Proposed Products for the Judiciary .....	5-7
Table 5-2: CD-ROM Products Used by the Judiciary .....	5-8
Table 5-3:CD-ROM Preferred Products for the Judiciary .....	5-8
Table 5-4: DVD Products Used by the Judiciary.....	5-8
Table 5-5: DVD Preferred Products for the Judiciary .....	5-8
Table 5-6: Scanning Products Used by the Judiciary .....	5-9
Table 5-7: Scanning Preferred Products for the Judiciary .....	5-9
Table 5-8: Printer Products Used by the Judiciary .....	5-11
Table 5-9: Printer Preferred Products for the Judiciary .....	5-11
Table 5-10: Server-Attached Local Disk Array Products Used by the Judiciary .....	5-12
Table 5-11: Server-Attached Preferred Products for the Judiciary.....	5-12
Table 5-12: NAS Products Used by the Judiciary .....	5-13
Table 5-13: NAS Preferred Products for the Judiciary .....	5-13
Table 5-14: SAN Products Used by the Judiciary .....	5-14
Table 5-15: SAN Preferred Products for the Judiciary .....	5-14
Table 5-16: Cable Products Used by the Judiciary .....	5-15
Table 5-17: Cable Preferred Products for the Judiciary.....	5-15
Table 5-18: Bridge, Router, and Switch Products Used by the Judiciary.....	5-15
Table 5-19: Bridge, Router, and Switch Preferred Products for the Judiciary .....	5-16
Table 5-20: Satellite Broadcasting Products Used by the Judiciary .....	5-17

Table 5-21: Satellite Broadcasting Preferred Products for the Judiciary..... 5-17  
Table D-1: Values in the Application Log Directory Structure..... D-4  
Table D-2: Hard Disk Configuration for 9.1-GB Disks ..... D-5  
Table D-3: Hard Disk Configuration for 18-GB Disks ..... D-5  
Table D-4: Root Space Allocation for 9.1-GB Disks ..... D-6  
Table D-5: Root Space Allocation for 18-GB Disks ..... D-6  
Table D-6: Application Directory Space Allocation ..... D-7  
Table D-7: Values in the Required Directory Structure ..... D-8

DRAFT

# Chapter 1 Introduction

## 1.1 Overview

The Information Resources Management Standard (IRMS) 701.1 establishes the Information Systems Architecture (ISA) as the framework of standards, guidelines, and design principles required to support the business needs and user requirements described in the *Long Range Plan for Information Technology in the Federal Judiciary*. The architecture design provides flexible automated solutions to address the evolving needs of the Judiciary and defines those components (hardware, software, and telecommunications) which lend themselves to the overall system design. The ISA promotes the seamless sharing of information in the most cost-effective and flexible manner.

IRMS 701.1 documents the ISA and also establishes the Technical Reference Model (TRM). The TRM is a framework of information technology standards and products. Subject to the conditions mentioned in the sections below and IRMS 701, the IT standards and products in this guideline are applicable to all new automation projects, products, and services. These guidelines should also be applied to existing products and ongoing projects to the greatest extent possible.

## 1.2 Purpose

The purpose of the TRM is to describe the guidelines and standards which form the basis for standardizing the Judiciary's information systems and for evaluating the architecture of proposed new judiciary information systems. As the TRM evolves, guidelines and standards will be established that when followed, will provide the ability for applications operating on the same or different platforms to communicate, exchange data, share common databases, or share a common service function without significant modification.

This document will be used to evaluate any proposal involving IT components and to direct the design, construction, deployment, and management of the technology aspects of those projects. The TRM is intended to help programs and projects work within a consistent technology framework throughout the Judiciary.

The TRM is not intended to limit the creativity of projects, but rather to make the outcomes more beneficial and manageable by adhering to architectural principles and IT best practices so that the many interrelated components of such a complex system are highly compatible and work together efficiently. This will ensure that the inventory of hardware, software, and skills can be used to the maximum benefit of the judiciary.

## 1.3 Scope

The September 1996 Judicial Conference initiated the following actions with respect to the Information Systems Architecture:

- 1) Adopted a policy that all projects initiated by the Administrative Office (AO) for national implementation or projects that are intended for multi-circuit use must conform with the ISA core requirements; adhere to the Automation Project Management Process; fully integrate with other projects and products; and utilize the existing communications and processing infrastructure of the ISA.

- 2) This standard does not apply to applications or other automation projects developed for local use by the courts and/or projects or applications acquired with local funds by the courts. However, where such projects or applications involve the sharing or exchange of data between courts within a circuit, or involve data that by statute or policy of the Judicial Conference must be provided to the Administrative Office, integration and connectivity among all intended users must be achieved.

The Assistant Director, Office of Information Technology (AD-OIT) has also determined that any project undertaken by the Administrative Office (AO) that utilizes funds from the Judiciary Information Technology Fund must conform to the ISA.

#### **1.4 Authority**

IRM standards are issued under the authority of the AD-OIT as the senior official for Information Resources Management for the Judiciary. This standard implements the policy set by the Judicial Conference of the United States at its September 1996 session.

#### **1.5 Responsibility**

##### **1.5.1 Assistant Director, Office of Information Technology**

The AD-OIT is responsible for directing the establishment and management of the Information Systems Architecture for the Judiciary, and for monitoring conformance.

##### **1.5.2 OIT - Chief Technology Officer (CTO)**

The CTO has responsibility for the administration and management of the ISA. Program responsibilities include the overall management and coordination of the ISA; all ISA-related updates to the Long Range Plan for Automation in the Federal Judiciary; and the development and maintenance of the TRM in support of the ISA.

##### **1.5.3 Project Manager**

The Project Manager has overall responsibility for ensuring that projects conform to the ISA. The Project Manager may rely upon the Development Manager and the Office of Information Technology (OIT) to provide ISA and TRM technical advice and support. Conformance requires the design of automation solutions and selection of products is compatible with the TRM.

##### **1.5.4 Development Manager**

The Development Manager assists the Project Manager in ensuring that final technical solutions and designs conform to the TRM.

#### **1.6 Intended Audience**

The TRM is intended for use by information technology managers, functional and project managers, developers, and their support contractors. The TRM will be used as a guideline for:

- Educating staff about IT technologies, standards, and the interrelationship between IT hardware and software components.
- Acquiring IT products and services.
- Developing and maintaining automated information systems.
- Designing an information systems architecture and information technology infrastructure.

## 1.7 References

The following IRMS technology standards documents provide additional information on the Information Technology Project Management Process and are located on the judiciary's intranet, J-Net. (Some of the included standards are now obsolete, but have been included for historical purposes.)

### IRMS 100.0 General

- 101.1 [Introduction & Overview \(Revised\)](#), March 1995
- 102.0 (Obsolete)
- 103.0 (Obsolete)

### IRMS 200.0 Managing Information Resources Series

- 202.0 [Volume 1, Chapter 8, Guide to Judiciary Policies and Procedures](#)
- 203.0 Evaluation of User Satisfaction, IRM Control & Adjustment (Obsolete)
- 204.0 Security Plan (Obsolete)
- 205.0 [Guidelines for Contingency Planning](#), September 1996
- 206.0 Disaster Recovery Plan for PCs, OIS and Small VS Systems (Obsolete)
- 207.0 Computer Security Standard (Obsolete)
- 208.0 [Novell 3.X Security Review](#), May 1997

### IRMS 300.0 Project Management Series

- 301.4 [Project Manager's Handbook](#), May 2004 (pdf)
- 302.1 [Project Management Plan](#), April 1999 (pdf)
- 303.1 [Joint Application Design Requirements Analysis](#), April 1999 (pdf)
- 304.1 [Risk Management Plan](#), December 2003 (pdf)
- 305.1 [Implementation Plan](#), December 2003 (pdf)
- 306.1 [Project Justification Statement](#), September 1999 (pdf)
- 307.1 [Functional Requirements Document](#), May 1999 (pdf)
- 308.1 [Alternatives Analysis](#), April 1999 (pdf)
- 312.0 [Project Transfer Agreement](#), December 2003 (pdf)

### IRMS 400.0 Development Series

- 402.0 [Configuration Management Plan](#), September 1996
- 403.0 [Software Quality Assurance Plan](#), September 1996

- 404.0 Test Plan & Test Results (Obsolete)
- 405.0 [General & Detailed Design](#), April 1995
- 406.0 [Database Design Specification](#), April 1995
- 407.0 [Application Software Specification](#), January 1995
- 408.0 [Software Application Operations Guide](#), November 1996
- 409.0 [Users Guide](#)

### **IRMS 500.0 Support Series**

- 502.0 Hardware Support Plan (Obsolete)
- 503.1 [Support and Maintenance Plan](#), September 2003 (pdf)
- 504.1 [Training Plan](#), April 2003 (pdf)

### **IRMS 600.0 Telecommunications Series**

- 601.0 [Telephone Service for Public Use](#), November 2001 (pdf)
- 602.0 Network Management (Obsolete)

### **IRMS 700.0 Architecture Series**

- 701.0 [Administration and Management of the ISA](#), July 1997
- 702.0 [Realtime Court Reporting Technical Standard](#), June 1997

### **IRMS 800.0 Data Administration Series**

- 801.0 Data Administration: Public Access; Backup & Recovery; Data Security (Obsolete)

## **1.8 Goals**

The goals of the TRM are to:

- Address the broadest possible range of common end-user functional requirements using common architectural components.
- Promote inter-operability of existing systems, systems under development, and systems in early planning stages.
- Provide for modular adaptability and expandability to permit straightforward matching of specific court requirements with local system designs conforming to the architectural model.
- Employ widely supported federal and industry standards to promote open systems solutions and facilitate extending the architecture to emerging technologies and products.
- Guide the development and acquisition of automated solutions.
- Promote reuse of existing infrastructure and automated solutions.
- Speed the delivery of information technology and lower its cost.
- Provide end users a consistent and integrated approach to applications and data.

In order to keep pace with changing technologies, the guidelines and standards defined in the TRM must be adaptable and be able to meet future developments and the changing needs of the Judiciary. The TRM is not static. The ISA provides for changes and additions to, as well as deviations from the standards, guidelines, and products defined in the TRM. The ISA processes by which waivers and changes are requested and reviewed are addressed in IRMS 701.1.

It is recognized that the goal of achieving an integrated, interoperable, and cost-effective technology architecture may be achieved through the application of several strategies. These strategies include:

- Integration of commercial off-the-shelf (COTS) products that conform to open industry standards.
- Custom-designed application development efforts that are based upon reference standards such as HTML.

This approach will provide the Judiciary maximum flexibility in defining the components of its architecture while achieving enterprise interoperability.

The Judiciary's installed base will be used as a contributing factor in determining future component architectures. As an example, the Judiciary's existing investment in a standard, national database and the impacts associated with migrating to another database product (e.g., data and file format conversions, training investments, maintenance costs, etc.), must be considered when defining the Judiciary's TRM.

## 1.9 Approach

The TRM is based on the fundamental concept and architecture contained in the Application Portability Profile (APP) developed by the National Institute of Standards and Technology (NIST)<sup>1</sup>.

The Open Group Architecture Framework (TOGAF)<sup>2</sup>, its referenced list of standards, and related standards will be used as references for the TRM as it is continually updated to incorporate emerging technologies. The Open Group, a self-defined vendor and technology-neutral consortium, sponsored an updated and amended version of the Department of Defense Technical Architecture Framework for Information Management (TAFIM), which was derived from the Institute of Electronic and Electronic Engineers (IEEE) Portable Operating System Interface (POSIX) 1003.0 model.<sup>3</sup> This version of the TAFIM is referred to as TOGAF.

Selected standards or specifications include those from national, international and federal standard organizations such as the American National Standards Institute (ANSI), International Organization for Standardization (ISO), IEEE, International Telecommunications Union (ITU), and NIST.

---

<sup>1</sup> National Institute of Standards and Technology, *Application Portability Profile (APP), the U.S. Government's Open Systems Environment Profile*. Version 3.0. NIST Special Publication 500-230. February 1996.

<sup>2</sup> For more information, reference <http://www.opengroup.org/togaf/>, Copyright © The Open Group, 2001, 2002.

<sup>3</sup> Department of Defense, *Technical Architecture Framework for Information Management, Version 3.0*. April 30, 1996. TAFIM was derived from the IEEE POSIX 1003.0 model - see Part IV, IEEE 1003.0.

Standards-based products adopted into the TRM are technically mature, stable, and available commercially for implementation. Commercial application software, which satisfies business needs and can be operated on the Judiciary's information infrastructure, is preferred over developing new application software.

### 1.10 Definition of Terms

- **Preferred Product**—A commercial hardware or software product that is designated as either a formal or informal standard-based product or tool that must be used for IT projects or to support ongoing IT operations. The designated *preferred product* will be used unless a waiver is approved to use another product. Refer to IRMS 701.1 for the waiver process.
- **Formal or de jure standard** —A standard that is designated by standards-setting or approving bodies such as ANSI, ISO, IEEE, or NIST.
- **Informal or de facto standard** —A standard that has emerged from popular usage. A de facto standard usually has no formal accreditation and is developed by either major vendors or consortiums. De facto standards are products that have achieved such a high degree of acceptance that they are widely accepted within industry and have been implemented in numerous commercial products.
- **Federal Information Processing Standard (FIPS)** —FIPS includes standards, guidelines, and technical methods that are developed by NIST. Some required standards or specifications have gone through rigid validation testing and accreditation. NIST frequently adopts standards that have been developed by national and international voluntary industry standards organizations. The use of voluntary industry standards enables the federal government to acquire commercially available off-the-shelf technology and to avoid the costs of developing its own standards.
- **International Organization for Standardization (ISO)**— Established in 1947, the ISO is a non-governmental organization with members from some 100 countries. Its mission is to promote the development of standardization and related activities in the world and to develop cooperation in the spheres of intellectual, scientific, technological, and economic activities. The scope of the ISO covers all standardization fields except electrical and electronic engineering, which is the responsibility of the International Electrotechnical Commission (IEC).

### 1.11 Document Organization

The TRM is organized as follows:

- **Executive Summary**  
Provides a document summary.
- **Chapter 1**  
Presents background, purpose, goals, intended audience, waiver procedure, definition of terms, and document organization.

- **Chapter 2**  
Identifies TRM components.
- **Chapter 3**  
Includes a detailed description of the Application Software Entity.
- **Chapter 4**  
Includes a detailed description of the Application Platform Entity.
- **Chapter 5**  
Includes a detailed description of the External Environment.
- **Chapter 6**  
Summarizes the Judiciary's Current and Target Architecture, and Profile of Standards.
- **Appendix A**  
Contains methods to access the TRM and points of contact.
- **Appendix B**  
Contains the Judiciary Profile of Standards.
- **Appendix C**  
Contains the Judiciary Profile of Preferred Products.
- **Appendix D**  
Details the configuration standards for AO procured servers.
- **Appendix E**  
Details the minimum workstation configuration.
- **Appendix F**  
Defines acronyms used in this version of the TRM.
- **Appendix G**  
References publications used to develop the TRM.

## Chapter 2 Model Components

### 2.1 Basic Components

The TRM includes two types of elements: entities and interfaces. The following are discussed:

Entities:

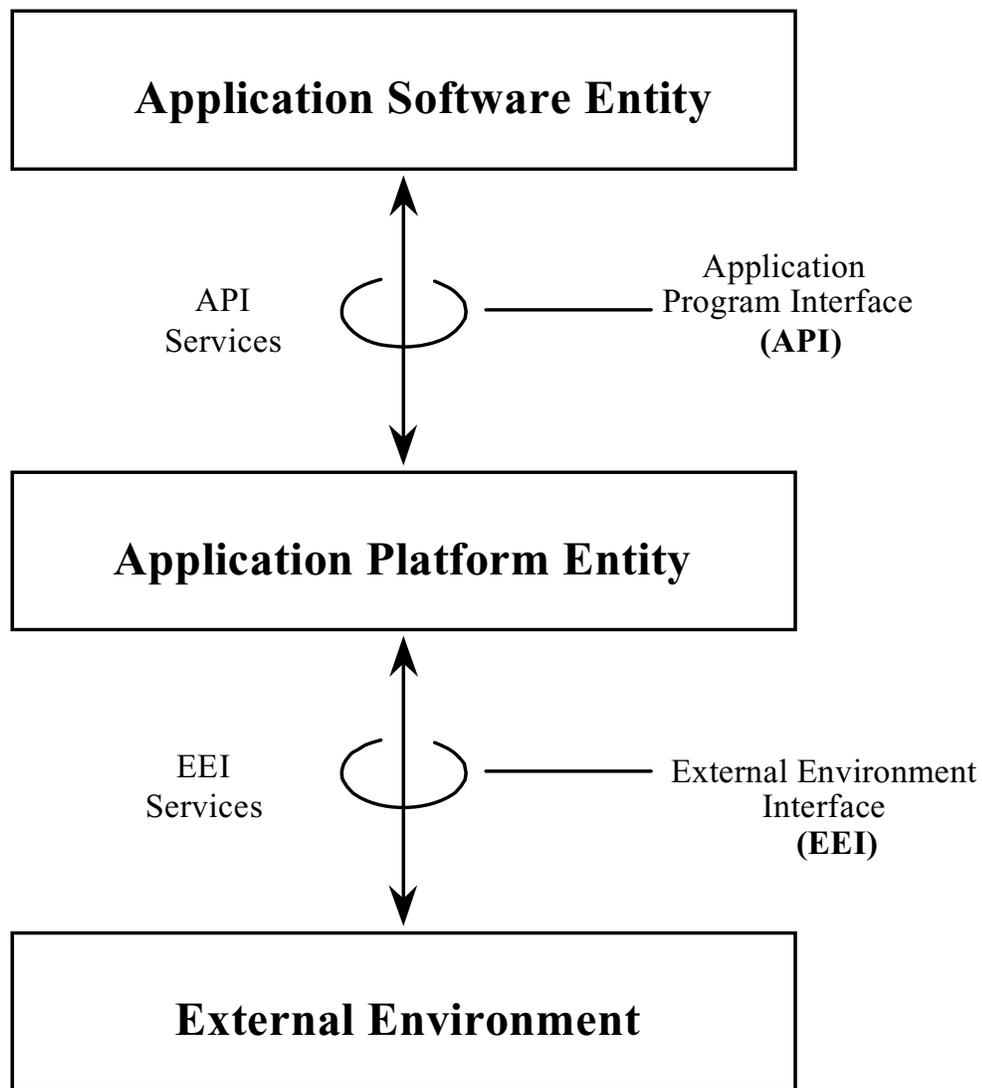
- Application Software Entity
- Application Platform Entity
- External Environment

Interfaces:

- Application Program Interface (API)
- External Environment Interface (EEI)

These elements lay the foundation upon which the Judiciary will build its information technology standards and select its standards-based, preferred products. The Judiciary will use these standards and standards-based products as guidelines for development and operation of its information technology infrastructure.

Figure 2.1-1 depicts the basic elements of the TRM. This figure is adapted from the POSIX Open Systems Environment Reference Model.



## Technical Reference Model Basic Components\*

\* Adopted from POSIX Open System Environment Reference Model

Figure 2.1-1: TRM High-Level Elements

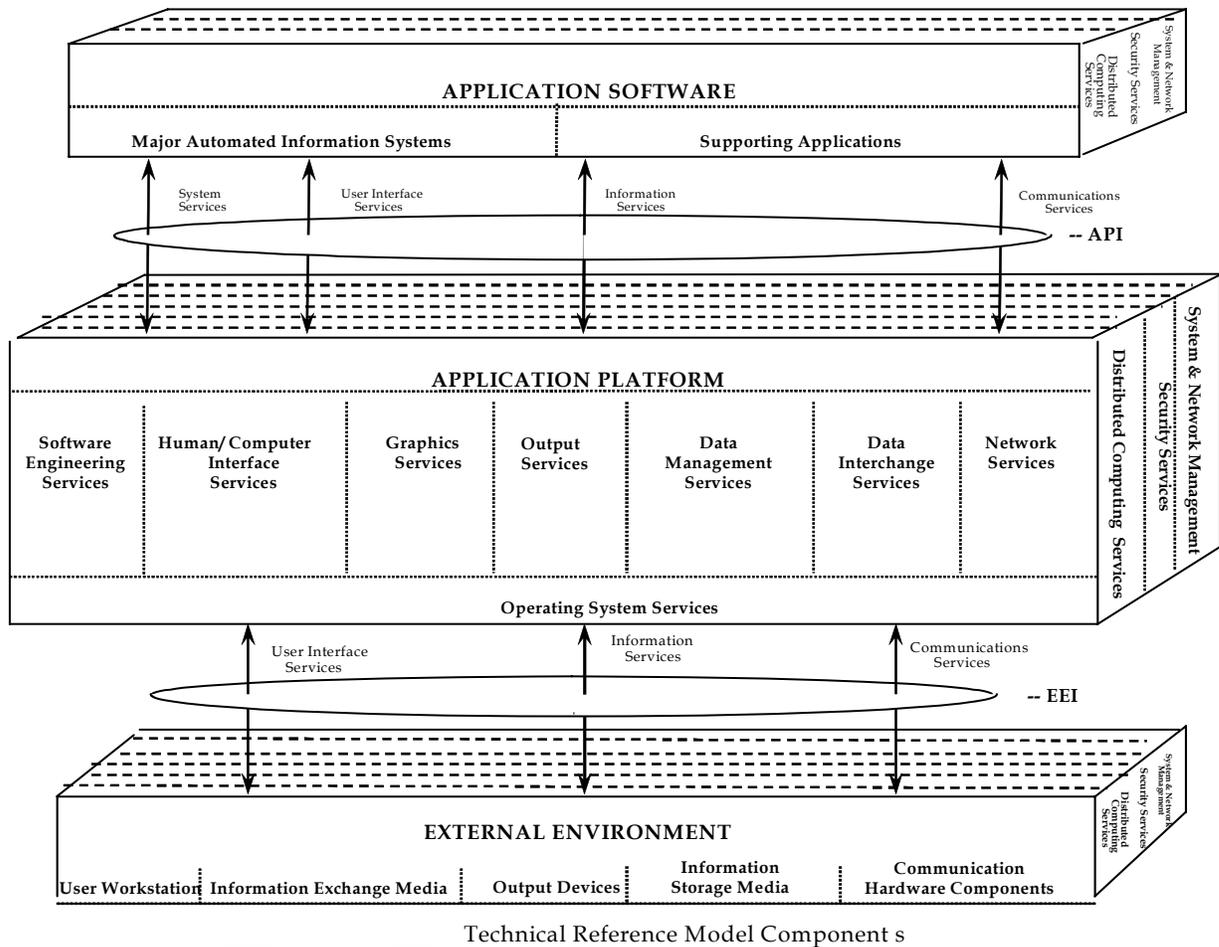
### 2.1.1 Principles

The model illustrates a user-supplier relationship: the application software is the user of services and the application platform entities are the suppliers. The API and EEI define the interfaces provided.

The Judiciary TRM illustrates the following principles:

- Software services are independent of hardware.
- All service areas interact with the operating system.
- System and Network Management Services, Distributed Computing Services, and Security Services are common to other services and pervade the service areas in one or more forms.

Figure 2.1-1 above depicts the high-level model and illustrates relationship between the basic components. Figure 2.1-2 illustrates decomposition of the basic components. Each component includes a set of lower-level components for which judiciary IT standards, interfaces, protocols, and products are defined.



**Figure 2.1-2: TRM Basic Components**

## 2.2 Component Descriptions

### 2.2.1 Entities

#### 2.2.1.1 Application Software Entity

Chapter 3 provides descriptions of the Judiciary applications included in the TRM Application Software Entity. Chapter 6 summarizes and illustrates the Current and Target Architecture using block diagrams, and shows how the Judiciary applications fit into the Target Architecture using the TRM model.

#### 2.2.1.2 Application Platform Entity

Components of the application platform described in Chapter 4 provide services or software resources for the application programs. The entity includes a comprehensive set of standards and products to support application portability, system interoperability, and scalability within and across automated information systems. The services included are:

- Server Hardware
- Operating System Services
- Software Engineering Services
- Human Computer Interface Services
- Data Management Services
- Data Interchange Services
- Graphics Services
- Computer-Based Interactive Training
- Output Services
- Network Services
- Videoconferencing
- Virtual LAN (VLAN)
- Voice Over IP (VoIP)
- Communications Protocols
- Security Services
- System and Network Management Services
- Distributed Computing Services

Table 2.2-1 shows the relationship between the each Application Platform Entity Service and the lower level service components, which are included in that service.

**Table 2.2-1: Application Platform Services**

SERVICES	LOWER-LEVEL SERVICE COMPONENTS
Server Hardware	Server Hardware
Operating System Services	Kernel Operations API Operating System Commands and Utilities Operating System Management Operating System Security
Software Engineering Services	System Development Methodology Business Process Re-engineering Data Modeling System Development Tools System Life Cycle
Human Computer Interface Services	Traditional Graphical User Interface Web Graphical User Interface Alternate User Interface Multimedia Interface Terminal Emulation

SERVICES	LOWER-LEVEL SERVICE COMPONENTS
Data Management Services	Metadata Repository Metadirectory Services Online Analytical Processing Data Extraction, Transformation, and Load (ETL) Tools Search Services Document Management Electronic Records Management (ERM) Web Content Management (WCM) Image and Multimedia Management Systems Database Management Systems (DBMS) Database Environments Data Management Security
Data Interchange Services	Financial and Human Resources Technical Standards Library Interchange Standards Unicode Standards Markup Languages Portable Document Delivery Format (PDF) File Compress Formats Office Automation File Formats Calendar Date and Ordinal Date Interchange Format Vector Graphics Raster Image Interchange Format Tag Image File Format (TIFF) Joint Photographic Experts Group (JPEG) Motion Picture Experts Group (MPEG) Electronic Data Interchange (EDI) Computer-Aided Design (CAD) Data
Graphics and Imaging Services	Graphical Kernel System
Computer Based Interactive Training	Computer Based Interactive Training
Output Services	Facsimile Transmission Service (fax) Compact Disk-Read Only (CD-ROM) Generation Service Digital Versatile Disc (DVD) Generation Service Digital Video and Film Generation Service Magnetic Tape Generation Service Plotting Service Print Service
Network Services	National Internet Gateways DCN/Backbone Configuration PacerNet Network File and Print Services Directory and Naming Services Domain Name Service (DNS) Electronic Mail, Message Services
Videoconferencing	Videoconferencing
Virtual LAN (VLAN)	Virtual LAN (VLAN)

SERVICES	LOWER-LEVEL SERVICE COMPONENTS
Voice Over IP (VoIP)	Voice Over IP (VoIP)
Communication Protocols	Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) Transmission Control Protocol/Internet Protocol (TCP/IP) Ethernet Wireless Local Area Network (WLAN) Frame Relay Asynchronous Transfer Mode (ATM) Dynamic Host Configuration Protocol (DHCP) Hypertext Transfer Protocol (HTTP) Uniform Resource Locator (URL) Multipurpose Internet Mail Extensions (MIME)
Security Services	Network Security Services Authentication Access Control Confidentiality, Integrity, and Non-Repudiation Audit Security Administration
System and Network Management Services	Network System Administration Help Desk Administration Communication Network Management Server Management Capacity Management and Performance Backup and Recovery Service
Distributed Computing Services	Distributed Computer Application Services Three-Tier Web-enabled DCA Model Distributed Computer Architecture Framework (DCAF) Intranet / Extranet Architecture Option Intranet Architecture Option Overview of DCAF Standards and Functional Elements Online Transaction Processing (OLTP) Distributed Computing Application Security Message Queuing Web Services

Chapter 4 provides detailed descriptions of the Application Platform Entity services and lower-level components. It also defines the standards and standards-based preferred products that the Judiciary will use to operate and develop its information technology infrastructure. Chapter 6.0 summarizes and illustrates the Current and Target Architecture using block diagrams, and shows how the Judiciary Application Platform Entity standards fit into the Target Architecture using the TRM model. Appendix C contains summarized a list of Application Platform Entity preferred products.

### **2.2.1.3 External Environment**

The external environment consists of those elements that are external to application software and the application platform. They include:

- User desktop workstations
- Information exchange media such as diskettes, CD-ROM, and data cartridges
- Information Storage Media such as magnetic data storage devices and disk array storage
- Communication hardware components such as fiber optics, unshielded twisted pairs, and telephone lines
- Output devices such as printers, plotters, CD-ROM writers, and film writers
- Security services
- System and network management services
- Distributed computing services

Chapter 5 provides descriptions of the External Environment Entity lower-level components. It also defines the standards and standards-based preferred products that the judiciary will use to operate and develop its IT infrastructure. Appendix D contains a summarized list of external environment entity preferred products.

## **2.2.2 Interfaces**

### **2.2.2.1 Application Program Interface (API)**

The application program interface is the interface between the application software and the application platform across which all services are provided. Its primary function is to support portability of application software. There are four types of APIs:

- System Services API, including APIs for Software Engineering Services, and Operating System Services.
- Human Computer User Interface Services API, including APIs for User Interface Services and Graphics Services.
- Information Services API, including APIs for Data Management Services and Data Interchange Services.
- Communication Services API, including APIs for Network Services.

### **2.2.2.2 External Environment Interface (EEI)**

The external environment interface is the interface that supports transfer of information between the application platform and the external environment. EEIs include:

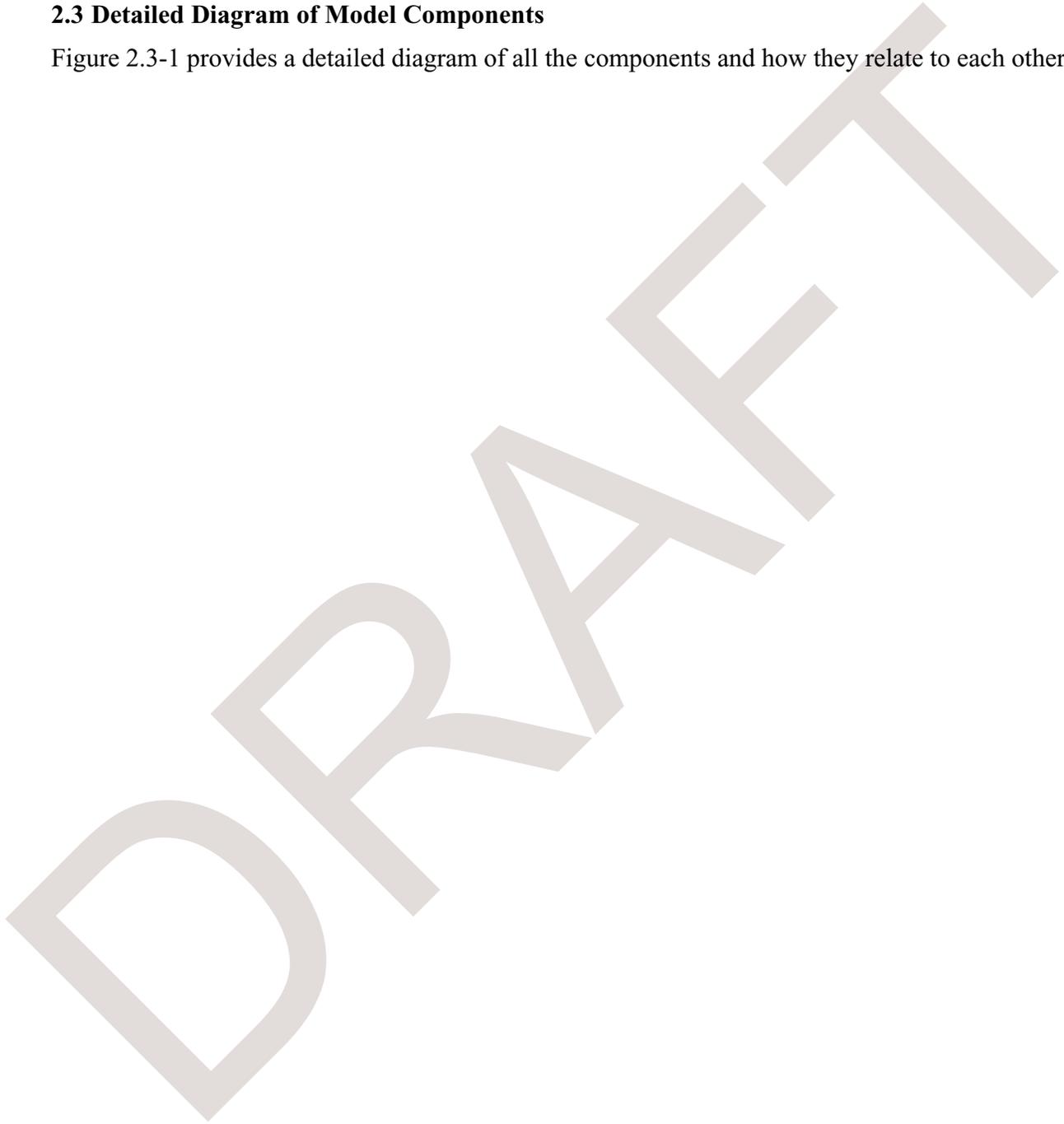
- Human Computer User Interface Services EEI such as computer monitors, keyboards, mice, and audio input/output devices and its format and syntax.
- Information Services EEI including external data storage and output device services.

- Communication Services EEI including protocols, syntax, and format.

Chapter 6.0 summarizes and illustrates the Current and Target Architecture using block diagrams, and shows how the interfaces fit into the Target Architecture using the TRM model.

### **2.3 Detailed Diagram of Model Components**

Figure 2.3-1 provides a detailed diagram of all the components and how they relate to each other.



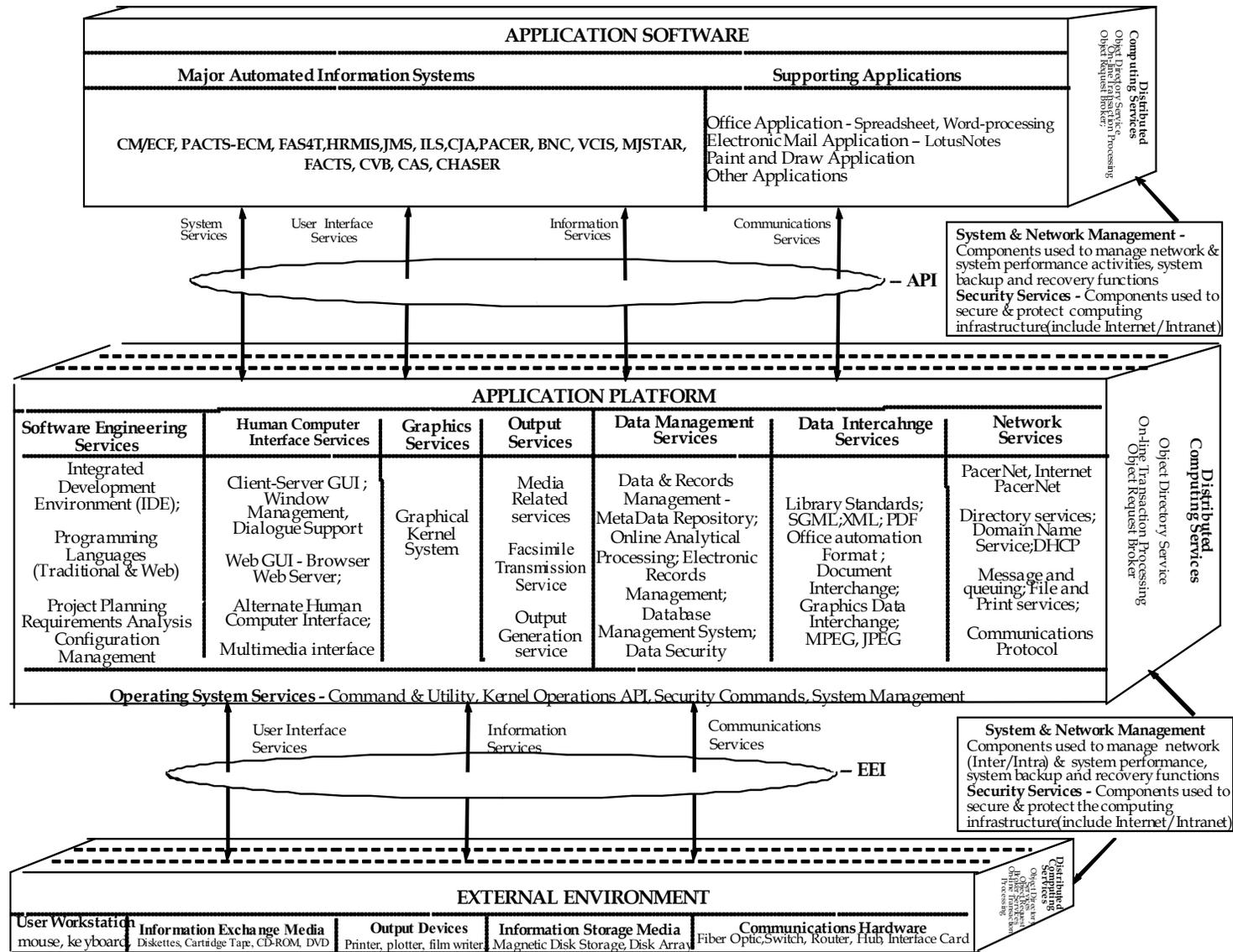
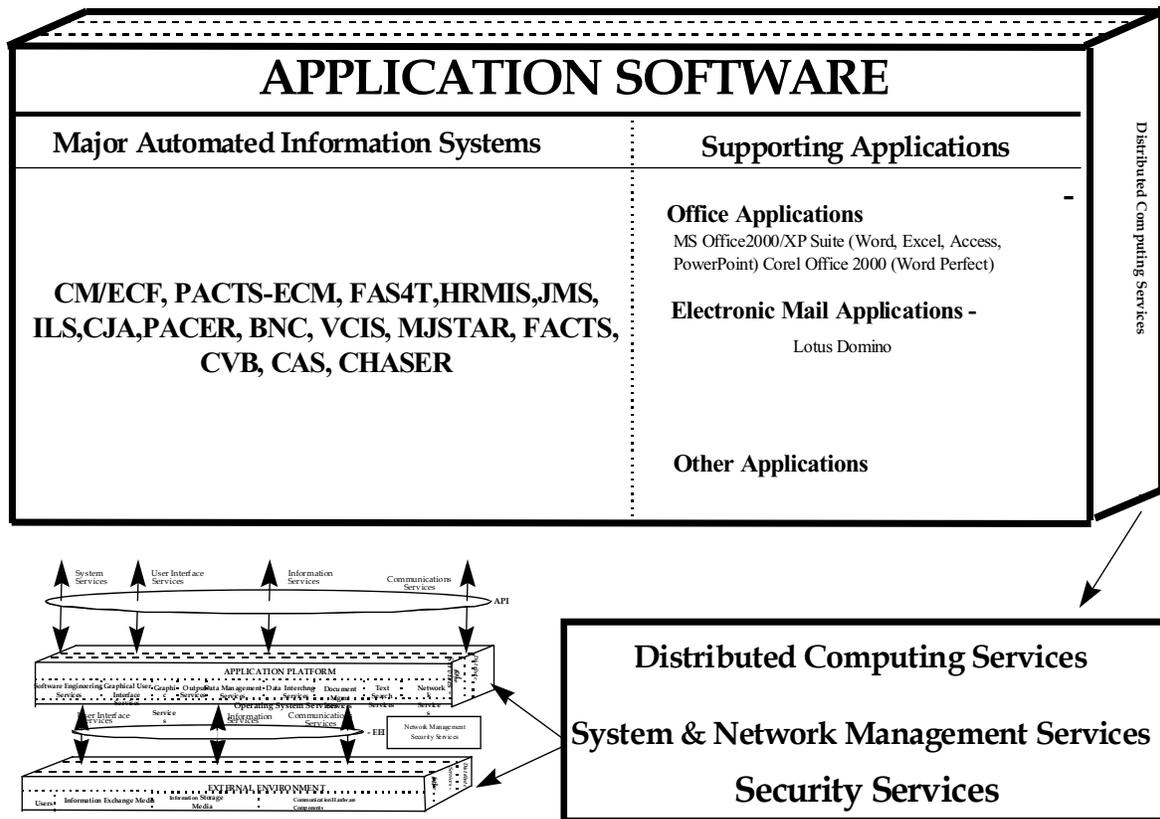


Figure 2.3-1: Judiciary Technical Reference Model Detail Level

# Chapter 3 Application Software Entity

## 3.1 Overview

Application software at the Judiciary consists of Automated Information Systems (AISs) and specialized applications as shown in Figure 3.1-1 below.



Summary of Application Software Entity

Figure 3.1-1: Diagram of Application Software Entity

The descriptions that follow provide high-level summaries of systems in operation and under development. The systems and applications operate within the purview of each of the Judiciary’s program areas. However, the descriptions that follow are organized into three functional categories: National Applications, Supporting Applications, and Local Applications.

## 3.2 National Applications

Applications that use these services include advisory council and group-sponsored applications supporting case management, noticing, jury management, administration, finance, personnel, payroll, statistical analysis, access to court records, and report generation. These applications are

hosted on nationally provided application servers and are accessible via the court's local area network.

### **3.2.1 CM/ECF**

Case Management/Electronic Cases Files (CM/ECF) is an AO-developed application currently hosted on Solaris 7 and 9 on Intel architecture-based platforms. Two implementations of CM/ECF currently exist, Bankruptcy and District. A third implementation, Appellate, is currently in design. CM/ECF will be hosted at 197 sites when fully deployed.

### **3.2.2 FAS4T and CJA**

Financial Accounting System for Tomorrow (FAS4T) and Criminal Justice Act system (CJA) are applications built for AO on top of AMS's Momentum application and 10 associated COTS products (see section 6.2) currently hosted on Solaris 7 on an Intel architecture based platform. FAS4T will be hosted at 94 sites when fully deployed. CJA is centrally hosted at AO. The migration of FAS4T and CJA to any of the target architectures will consist primarily of porting the AO custom software.

### **3.2.3 HRMIS**

Human Resources Management Information System (HRMIS) is an application built on top of PeopleSoft with some supporting COTS products (see section 6.2) currently hosted on HPUNIX (UNIX). HRMIS is centrally hosted at AO.

### **3.2.4 ILS**

Integrated Library System (ILS) consists of the COTS application Unicorn currently hosted on Solaris 7 on Intel. ILS is fully deployed at 13 sites. The Unicorn application is only available on Solaris, so the only viable target architecture for ILS is Sun Solaris 8 SPARC.

### **3.2.5 JMS**

Jury Management System (JMS) is a client-side application. The only server component of JMS is an Informix database currently hosted on Solaris 7 on an Intel architecture based platform. JMS is fully deployed at 89 sites.

### **3.2.6 PACER**

Public Access to Court Electronic Records (PACER) is an AO-developed application currently hosted on Solaris 6 on an Intel architecture-based platform. Central Violation Bureau (CVB) is an AO-developed application currently hosted on Solaris 7 on an Intel architecture-based platform. Both applications are centrally hosted at the AO.

### **3.2.7 PACTS**

Probation and Pretrial Offices Services Automated Case Tracking System (PACTS) is an AO-developed application currently hosted on Solaris 7 on an Intel architecture-based platform. PACTS will be hosted at 94 sites when fully deployed. The migration of PACTS to any of the target architectures will consist primarily of a porting effort of varying complexity.

### **3.2.8 CHASER**

Chambers Access to Selected Electronic Records (CHASER) is an automated case information retrieval system for district court judges and their staffs. It provides judges and chambers staff with immediate access to electronic docketing information, as well as general statistical reports on their caseloads. The system is designed to be simple for the user to operate, yet flexible to meet individual case management needs. Four categories of information are available: docket reports, case inventories, motion tracking, and statistical reports.

### **3.2.9 CJA**

Criminal Justice Act System (CJA) processes payments for all attorneys, expert witnesses, and other court-related services for federal defendants. Statistical and program data for this system reside on the Judiciary Central Processing System, located in Washington D.C.

### **3.2.10 CAS**

Central Accounting System (CAS) provides ongoing support to the AO and the federal courts and is the official repository of financial information for the Judiciary. It provides such information as recording the appropriation amounts approved by Congress; providing funds control over the budget authority given to the AO program divisions, the courts, and other units of the judiciary; recording all obligations and expenditures; generating purchase orders; and writing checks. In addition, CAS produces the financial reports required by Treasury and the AO program divisions, as well as some reports used by various court units.

### **3.2.11 CVB**

Central Violations Bureau (CVB) processes over 95 percent of all petty offense violations and some misdemeanor violations that occur on federal properties such as national parks and military bases. The system currently operates in San Antonio, Texas.

### **3.2.12 NewFACTS**

New Facilities Automation for the Courts (NewFACTS) is an application designed to support the management of the judiciary's space inventory. Featuring online query and report generation capability, NewFACTS will serve, when fully implemented, as a management tool to track and manage real property projects. It will also support the management of funding for real property acquisitions, construction and repair projects.

### **3.2.13 MJSTAR**

Magistrate Judges Statistics and Reporting System (MJSTAR) seeks to integrate the statistical reporting for magistrate judges with the Integrated Case Management System (ICMS), allowing for the elimination of the manual JS-43 monthly workload reporting form. Planned activities for this project include the design of a module to extract data from ICMS, and perhaps from other sources, in order to accurately and comparatively depict the workload of magistrate judges in a district.

### **3.2.14 VCIS**

Voice Case Information System (VCIS) was developed to handle the millions of telephone inquiries concerning specific bankruptcy cases. It uses an automated voice response system to read bankruptcy case information directly from a court's database in response to touch tone inquiries. The caller gets this information without charge, except for any long distance telephone charges. This system's success has led to the development of a prototype of VCIS for appellate courts.

### **3.2.15 BNC**

Bankruptcy Noticing Center (BNC) utilizes electronic noticing because it is a more efficient and expedient way to meet the clerks' legal requirement to notice events in bankruptcy cases.

## **3.3 Supporting Applications**

Supporting applications are those commonly used applications used across the judiciary to support electronic mail, office operation, and other applications.

### **3.3.1 Electronic Mail Applications**

Lotus Domino/Notes electronic mail product has been implemented as the judiciary-wide e-mail system. It replaced the previous cc:Mail infrastructure and other e-mail systems installed throughout the courts. Lotus Professional Services proposed Windows NT4 on an Intel platform as the product's platform for implementation. This decision was based on such considerations as the product's operating environment requirements, the commercial availability and market presence of the various platforms, the scalability and expected performance of the various platforms under projected usage scenarios, expected e-mail traffic over the DCN wide-area network, and platform configuration cost.

Approximately 140 servers were deployed based upon the expected numbers of users served at each court location, with consideration given to DCN connectivity and capacities. To comply with this design, court units within a district share physical mail server resources. Platform-sharing relates only to the physical location of the mail servers; all court units will still have local control, to the extent possible, over the logical organization of their email databases (including directories, mail lists, e-mail management, policies, etc.), regardless of the physical placement of those databases.

### **3.3.2 Office Applications**

Office applications support day-to-day operations: word processing, spreadsheets, and graphics presentations. WordPerfect is the standard word processor within the judiciary. The Courts also uses various versions of the Microsoft Office suite, including 2000 and XP. The Microsoft Office suite of applications includes Word, Excel, PowerPoint, and Access. Users access these services from desktop workstations that communicate with servers on the DCN.

## **3.4 Local Applications**

This section outlines major automated information systems that provide information and guidance regarding various AO's functions and procedures such as: Executive Support Systems,

Financial Information Systems, Information Dissemination Systems, and Office Automation Systems.

### **3.4.1 Executive Support Systems**

Executive Support Systems provide an automated, integrated, and centralized approach for performing AO Human Resources key functions. Executive Support Systems make critical human resources data available as quickly as possible to AO staff and policy makers. The following systems serve the functions of planning, controlling and decision-making at the executive management level.

#### **3.4.1.1 Correspondence Control Management System (CCM)**

The objective of CCM is to provide the AO with the ability to process, route, and track correspondence. Staff members who depend on this software include the Director's Office, the Associate Director's Office, and the Executive Correspondence Staff, as well as other offices throughout the AO. The product allows AO Offices to track where correspondence is coming from, who it has been routed to, where the correspondence currently resides, who has been tasked, and if the tasking is open or closed. The product provides office-wide document tracking, and simplifies and streamlines the executive document review, correction, and approval process.

#### **3.4.1.2 OnTime**

The OnTime application is used to generate a Trifold report which is essentially a calendar. The application is used to maintain the following type of information for the Director and the Associate Director of the AO: appointments, tasks, upcoming events, work records, and an area for notes which may be used to keep track of expenses.

#### **3.4.1.3 Major Initiatives Project or Study System (MIPS)**

MIPS is used to track management initiatives and action items. The system is used to generate information pertaining to a division's annual business plan including goals, major projects, work activities, schedules, and milestones. Each division prepares the status report based upon the execution of its business plan. The primary functions of MIPS are the following:

- Collect Division Initiative Reports (scalable for the entire AO)
- Consolidate Reports
- Generate the Consolidated Initiative Report which is formatted just as with the current manual process
- Generate the Division Initiative Report when reports are entered directly into the MIPS system

#### **3.4.1.4 Judiciary Executive Management System (JEMS)**

JEMS is designed to make critical human resources data available as quickly as possible to AO staff and policymakers. JEMS data comes from the judiciary's main personnel files and represents the most current information. Since the process of transferring data to JEMS is complex, the update is scheduled on a regular biweekly cycle coinciding roughly with the payroll calculation cycle.

### **3.4.1.5 Personnel Activities Tracking System (PATS)**

The Personnel Activities Tracking System (PATS) is designed for the AO Personnel Division (AOPD) of the AO. PATS is the central repository for personnel case documents processed by the AOPD. These case documents are updated by Human Resources Specialists and Personnel Management Assistants. The system also allows the AOPD to create and process personnel requests from other AO offices.

### **3.4.2 Financial Information Systems**

AO's Financial Information Systems generate and route financial and non-financial data between the courts and the Budget Division and the Payroll Support Branch. One of the primary functions of AO's Financial Information Systems is to provide Budget Division staff with the ability to manage the budget process, including reports and data entry for the Annual Budget Call Appeals, Allotment Simplification, and Supplemental Requests.

AO's Financial Information Systems also provide the Budget Division staff with the ability to process recommendations on all funding requests and review Reprogramming Requests.

#### **3.4.2.1 Integrated Court Information System (ICIS)**

The purpose of ICIS is to generate and route financial and non-financial data between the courts and the Budget Division. The ICIS LAN is a sub-network of the DCN which provides connectivity to major applications and resources located among each court within the Federal Judiciary. The primary functions of ICIS are the following:

- Provide the Budget Division staff with the ability to process recommendations on all funding requests and review Reprogramming Requests.
- Provide the Budget Division staff with the ability to process notifications of significant transactions and late notices to court and AO staff.
- Provide AO allocation holders with the ability to manage funds and assist Budget Division staff in performing non-financial tasks.
- Provide the Budget Division staff with the ability to manage the budget process, including reports and data entry for the Annual Budget Call Appeals, Allotment Simplification, and Supplemental Requests.
- Provide the courts with the ability to enter and submit funding requests.
- Provide the courts with the ability to submit electronic status fund requests and other reports.
- Provide the courts the ability to retrieve payroll and other financial data.
- Provide the courts the ability register official e-mail addresses used by the AO and Lotus Notes.

#### **3.4.2.2 Quarterly Review Application**

The Quarterly Review Application is required to organize financial data and produce information for use by the Associate and Assistant Directors in their exercise of financial management oversight. At the end of the first, second, and third quarters of the fiscal year, senior managers review all significant aspects of judiciary financial operations in the Salaries and Expenses, Court Security, Defender Services, and Fees of Jurors accounts.

Management is provided with information regarding the availability of funding for each program and what funds will be available to carry forward to the next fiscal year. A summary of this review is forwarded to the Director for his information. Information is made available at the Budget Object Class (BOC) and organization code level, and summarized to the Assistant Director and fund levels.

### **3.4.2.3 Architectural Statements of Qualifications (AESOP)**

The objective of AESOP is to provide an efficient automated approach for tracking architectural engineer statements of qualifications in accordance with the Brooks Act. The System enables staff from the Office of Facilities and Security to store, update, delete, and retrieve critical data pertaining to architectural engineering statements of qualifications. The automated solution increases speed and efficiency of the research process by shortening the time required for search and retrieval, targeting search criteria more accurately, and providing both old and new data pertaining to architectural engineering statements of qualifications. The system is also instrumental in acquiring timely architectural engineering services to the Federal Courts.

### **3.4.2.4 Automated Form AO-15 Requisition**

The Automated Form AO-15 Requisition System provides the capability to submit AO-15 procurement requests, process them through the approval chain, and track the status AO-15 procurement requests. The AO-15 system allows staff to accomplish the following:

- Electronically submit or advance request documents to the next status in the approval chain.
- Save and edit request documents before advancing to the next stage in the approval chain.
- Electronically attach documents related to justification of the AO-15 request document.
- E-mail is used to:
  - Automatically notify the next participant in the approval chain
  - Link directly to an AO-15 request document
  - Receive modification instructions
  - View instantly the approval chain status of an AO-15 request document
  - View and track AO-15 request documents by organizational and inventory data
  - Perform a text search of AO-15 documents

### **3.4.2.5 Garnishment Information System (Garnisys)**

The purpose of the Garnishment Information System (GARNISYS) is to provide the AO's Payroll Support Branch with the ability to process, track, and make payments for writs that are served on Judiciary employees throughout the United States, and its territories and possessions, in accordance with Section 5502a of Title 5, United States Code. Enacted in 1993, this permits the pay of Federal employees to be garnished for any purpose through legal process issued by a competent authority with the United States. Timeliness and accuracy are critical factors, because the AO will be responding to court orders as well as withholding portions of employees' pay.

## **3.4.3 Information Dissemination Systems**

Information Dissemination Systems are used to develop, maintain, and disseminate a diversified portfolio of information (e.g., memorandums to court personnel, legal documents) within the AO

and to court personnel within the federal courts. These efforts are supported by the following systems:

#### **3.4.3.1 E-Mail Broadcaster**

E-Mail Broadcaster is used by the AO to send out mass communications to the courts and the AO Senior Staff. The E-Mail Broadcast System can send mailings to all Unit Executives, Chief Deputies, Probation Chiefs, and other court personnel by category. E-Mail Broadcaster is used to send messages and attachments to groups of individuals in the judiciary via the Intranet using Infoweb. The primary functions of E-Mail Broadcaster are the following:

- Allow staff to send hundreds of e-mails to groups of judiciary officials.
- Provide flexibility to chief judges and court executives in deciding how they wish to manage electronic mail.
- Send out broadcast verifications as part of the E-Mail Broadcast System.

#### **3.4.3.2 Online Legal Information Environment (OLLIE)**

OLLIE provides an efficient method for filing, searching, retrieving, and editing legal documents within the Office of General Counsel. The System will allow researchers to perform a search for documents using meta-tags, full-text search or both, and will return a result set of relevant documents and attachments, as well as related responses. OLLIE includes features that WestLaw does not offer (e.g., ability to add workflow, ability to link responses and related documents to a retrieved document, ability to maintain document structure).

#### **3.4.3.3 PeopleFinder**

The purpose of PeopleFinder is to provide the federal judiciary and the AO a single automated solution for producing and maintaining the following directories:

- Federal Judiciary Court Directory
- Administrative Office of the U.S. Courts Directory
- Defender Services Directory
- Directory of U.S. Probation and Pretrial Officers

These directories are used primarily by the federal judiciary, with limited access by the executive and legislative branch agencies, and the public. PeopleFinder is designed to provide an automated solution for producing, updating, and printing the various administrative directories for the Judiciary and AO, while streamlining and enhancing user accessibility.

#### **3.4.3.4 Records Management Tracking System (RMTS)**

The proposed RMTS will provide automated support and controls for the transfer of inactive records from the AO to the Federal Records Center (FRC). RMTS will track records through the records management life cycle from creation to destruction. RMTS will automate the following activities in the transfer process: requesting an accession number; generating and printing labels for boxes and folders, generating and printing box inventory reports, and tracking the location of boxes and folders.

### **3.4.3.5 Guide Enhancement Project**

The proposed system will provide the capability to manage the full document life-cycle for producing and publishing changes to the *Guide to Judiciary Policies and Procedures*. It will provide the capability to manage the full document life-cycle for producing and publishing changes to the Guide. A web site will also be developed to include procedures, standards, and guidance for making changes to the Guide.

The proposed system will accomplish the following:

- **Version Control:** A version control procedure is needed in order to keep track of the status of each transmittal in terms of draft, final etc. for each electronic version of the Guide. Version control is also needed in order to validate that correct information is being posted to the J-Net.
- **Access Control:** Where multiple versions of a document are being recorded, the system needs to track the relationships between those versions, to track from what document version (or versions) a given transmittal was created, who made the changes, and what those changes were.
- **Workflow:** Procedures need to be defined and automated in order to reduce the time frame for reviewing, approving, and disseminating changes to the Guide.

### **3.4.4 Office Automation Services**

Office Automation (OA) Services provide AO personnel with many capabilities such as access to electronic mail, printing services, and various applications. AO personnel access these services from desktop workstations that communicate with servers and gateways on the AO's network. The Office Automation Suite includes applications that support day-to-day operations, such as word processing (e.g., WordPerfect), spreadsheet, and graphics presentation. AO uses the Microsoft Office suite of applications, including Microsoft Word, Excel, and PowerPoint.

#### **3.4.4.1 Electronic Mail Services**

These services include electronic mail and groupware tools used to support group communication and activities across AO offices. Lotus Notes is the AO's e-mail application. Lotus Notes provides software to organize, integrate, and manage electronic mail, calendars, tasks, contacts, documents, and scheduling. Refer to electronic mail services under network services for further information.

#### **3.4.4.2 Enterprise Facsimile Transmission Services**

These services enable AO users to view and edit faxes online and route them throughout the enterprise.

#### **3.4.4.3 Enterprise Print Services.**

These services provide the hardware and software that supports the printing of AO documents. Enterprise Print Services supports standards-based printers from multiple vendors and includes software that enhances AO's ability to effectively administer enterprise printers.

#### **3.4.4.4 Enterprise-Wide Login Services**

The Enterprise-Wide Login Services provide enterprise-wide login authentication and access control mechanisms for AO's network and the systems operating on the AO's network. The primary Enterprise-Wide Login objectives are to provide authentication and access control mechanisms, confidentiality support, reduction of multiple log-in processes, and support for the development of future sensitive systems operating on the AO's network.

## Chapter 4 Application Platform Entity

### 4.1 Overview

The components of the application platform provide services or resources for application programs. The AO is identifying a comprehensive set of standards and products for the following services:

- Server Hardware
- Operating System Services
- Software Engineering Services
- Human/Computer Interface Services
- Data Management Services
- Data Interchange Services
- Graphics Services
- Computer-Based Interactive Training
- Output Services
- Network Services
- Videoconferencing
- Virtual LAN (VLAN)
- Voice Over IP (VoIP)
- Communication Protocols
- Security Services
- System and Network Management Services
- Distributed Computing Services

For each major service the following information is provided when available:

- Service Description
- Required Standards
- Products Used by the Federal Judiciary
- Preferred Products for the Judiciary
- Proposed Products for the Judiciary
- Future Products to Which the Judiciary Will Evolve

Specific standards and products may apply to more than one application platform service so it may be necessary to review several related services in order to find all cases where a particular standard or product applies. This document is intended as both a hardcopy desk and online reference.

There are four different categories for products: Used, Preferred, Proposed, and Evolve:

- Used: Contains all known products that are presently in use for Judiciary projects.
- Preferred: These products are the Judiciary standards. They are a subset of products in the used category.
- Proposed: Proposed products are products that are to be considered for future use by judiciary projects. The ISA defines the process that evaluates and approves or rejects products for future use.
- Evolve: Products that are known to be future Judiciary standards but are not in use or project plans today. There is likely to be a date for each product when projects should start using this new product. Once a product has selected for a Judiciary project it moves from Evolve to Used and Preferred.

A summary list of all Reference Standards is found in Appendix B. Appendix C includes a summary list of preferred products.

Figure 4.1-1 provides a diagram of the Application Platform Entity for the AO.

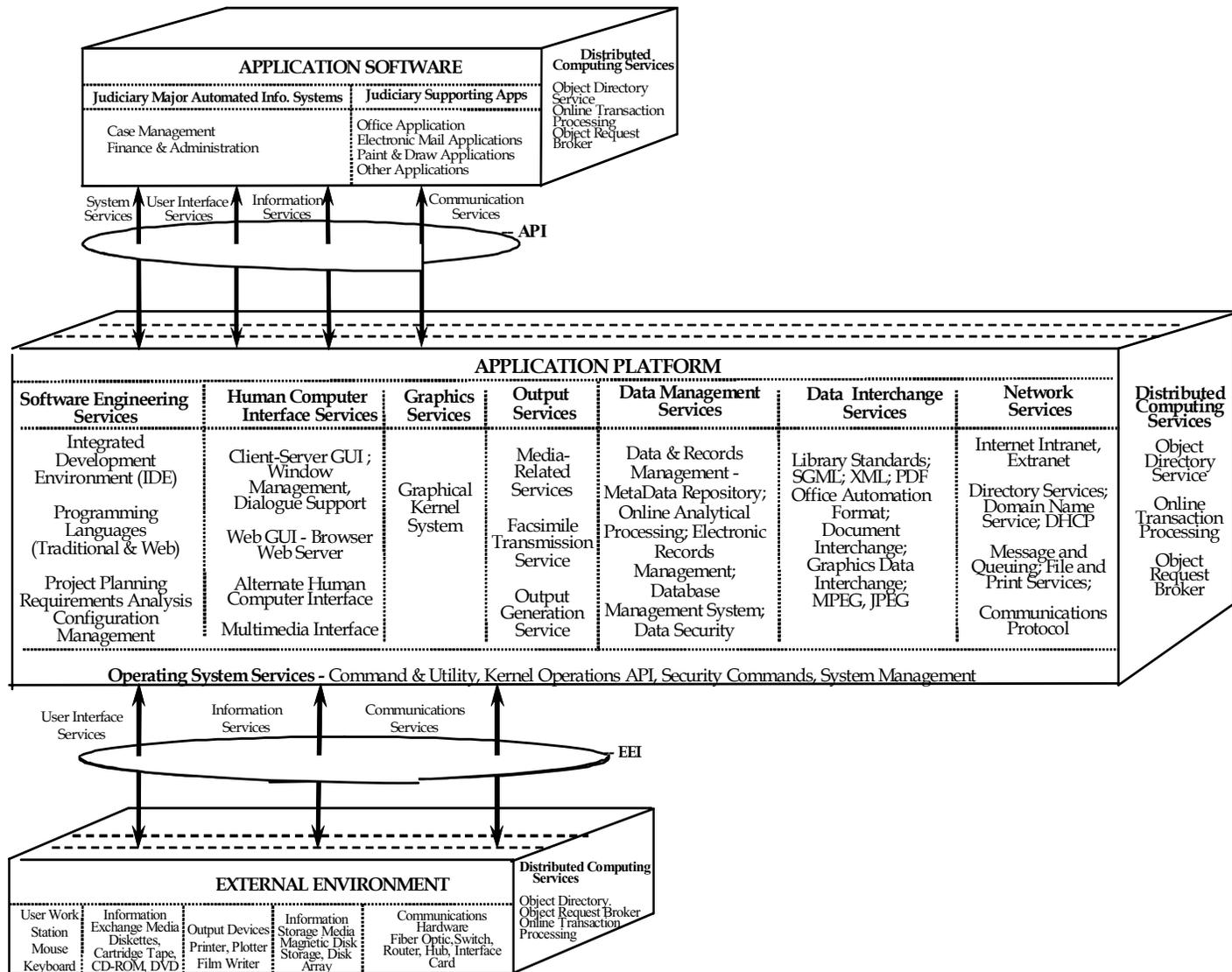


Figure 4.1-1: Application Platform Entity Diagram

## 4.2 Server Hardware

Please see Appendix C.

## 4.3 Operating System (OS) Services

Operating system services describe the following areas:

- Kernel Operations Application Program Interface (API)
- Operating System Commands and Utilities
- Operating System Management
- Operating System Security

### 4.3.1 Kernel Operations API

Kernel operations provide low-level services necessary to create and manage processes, execute programs, define and communicate signals, define and process system clock operations, manage files and directories, and control input/output processing to and from external devices. An ISO/IEC POSIX-compliant operating system facilitates hardware and operating system independence and maximizes source code portability.

*Required Standards:*

- International Standard ISO/IEC 9945-1: 2003, Information technology – Portable Operating System Interface (POSIX)—Part 1: Base Definitions (Incorporates IEEE Std 1003.1-2001/Cor1-2002, Standard for Information Technology—Portable Operating System Interface (POSIX) –Technical Corrigendum 1)  
[http://standards.ieee.org/reading/ieee/std\\_public/description/posix/](http://standards.ieee.org/reading/ieee/std_public/description/posix/)  
<http://standards.ieee.org/regauth/posix>  
<http://www.opengroup.org/austin/>

**Table 4.3-1: Kernel Operations Products Used by the Judiciary**

Vendor	Operating System	Hardware Platform	Scope
<a href="#">Hewlett Packard</a>	HP-UX v10.x, HP-UX v11.x	HP 9000	HRM <sup>1</sup>
<a href="#">Microsoft</a>	Windows 95 / 98 / ME, Windows NT 4.0 <sup>2</sup> , Windows 2000 / XP / 2003	x86-based workstations / servers	ALL
<a href="#">Novell</a>	NetWare 4.11 / 5.1/5.2 SuSE	x86-based servers	ALL
<a href="#">Red Hat</a>	Enterprise Linux	x86-based servers	ALL
<a href="#">Sun Microsystems</a>	Solaris 2.x; Solaris 7 (SunOS 5.7), Solaris 8 (SunOS 5.8), Solaris 9 (SunOS 5.9)	x86-based servers <sup>3</sup> , Sun workstations, Sun servers	ALL

<sup>1</sup> HRM: PeopleSoft Servers

<sup>2</sup> Windows 95/98/ME/NT 4.0: No further development should be done on these platforms.

<sup>3</sup> Solaris on x86: No further development should be done on this platform.

Vendor	Operating System	Hardware Platform	Scope
<a href="#">IBM</a>	OS390	IBM Multiprise Series 2000 Model 224	AO <sup>1</sup>
<a href="#">Hewlett Packard</a>	Windows CE	HP iPAQ	PCT <sup>2</sup>
<a href="#">Palm</a>	Palm OS	Palm	

**Table 4.3-2: Kernel Operations Preferred Products for the Judiciary**

Vendor	Operating System	Function	Judiciary Platform	Scope
<a href="#">Red Hat</a>	Enterprise Linux 4.x	Enterprise servers	x86-based server	ALL
<a href="#">Microsoft</a>	Windows XP	Desktop workstation	x86-based workstation	ALL
<a href="#">Microsoft</a>	Windows XP	Notebook	x86-based notebook	ALL
<a href="#">Hewlett Packard</a>	Windows CE	Handheld	HP iPAQ	PCT <sup>2</sup>
<a href="#">Palm</a>	Palm OS	Handheld	Palm	

**Table 4.3-3: Kernel Operations Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Red Hat</a>	Enterprise Linux 4.x	Desktop workstation	x86-based workstation	ALL
<a href="#">Red Hat</a>	Enterprise Linux 4.x	Notebook	x86-based notebook	ALL

### 4.3.2 Operating System Commands and Utilities

Commands and utilities include functions such as comparing, displaying, and printing file contents, editing files, pattern searching, evaluating expressions, logging messages, moving files between directories, sorting data, executing command scripts, scheduling signal execution processes, and accessing environment information.

The operating system (OS) commands and utilities define a source-level interface to users, shell scripts, and common utilities for application programs that conform to the POSIX standard. Shell script programming allows system programmers or operators to easily create and write portable command files. The script files provide operators with mechanisms to combine functions that are usually performed by separate and individual utilities.

*Required Standards:*

- ISO/IEC 9945-3:2003, Information Technology - Portable Operating System Interface (POSIX) - Part 3: Shell and Utilities  
<http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=38791&ICSI=35&ICS2=60&ICS3=>

<sup>1</sup> AO: Mainframe

<sup>2</sup> PCT: Mobile Data Access

<http://standards.ieee.org/regauth/posix/index.html>

*Products Used by the Judiciary:* The majority of operating system commands and utility functions are packaged and documented with the operating system, and are not separately identified. The following separately purchased utilities are also used.

**Table 4.3-4: Additional OS Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Sun Microsystems</a>	Solaris OS	Operating System Utilities	x86-based servers	ALL
<a href="#">Microsoft</a>	Windows NT, 2000	Operating System Utilities	x86-based servers	ALL
<a href="#">Red Hat</a>	Linux Advanced Server	Operating System Utilities	x86-based servers	ALL
<a href="#">Symantec</a>	Norton Utilities 4.0	Workstation disk maintenance	x86-based workstation, Windows 95, 98, ME, ME, NT, 2000, XP	ALL
Open Source	SSH	Encrypted terminal connections	x86-based servers, Linux	ALL

**Table 4.3-5: OS Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Red Hat</a>	Linux Advanced Server	Operating System Utilities	x86-based servers	ALL
Open Source	SSH	Encrypted terminal connections	x86-based servers, Linux	ALL

### 4.3.3 Operating System Management

The operating system management services provide system administrator functions such as software administration, user and group account management, and printing interfaces. The services are based on detailed specifications for packaging, distribution, installation, configuration, and removal of software in distributed systems; adding, modifying, and deleting user and group accounts, an interface to manage passwords associated with accounts; and a detailed printer interface specification. Backup utilities are also required to provide recovery mechanisms for major and minor problems.

*Required Standards:*

- ISO/IEC 15068-2:1999, Information Technology - Portable Operating System Interface (POSIX) System Administration - Part 2: Software Administration  
[http://standards.ieee.org/reading/ieee/std\\_public/description/posix/](http://standards.ieee.org/reading/ieee/std_public/description/posix/)  
<http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26362&ICSI=35&ICS2=60&ICS3=>  
[http://ieeexplore.ieee.org/xpl/abs\\_free.jsp?isNumber=16678&prod=STD&arnumber=770132&arSt=ared=&arAuthor=&arNumber=770132&a\\_id0=770132&count=1](http://ieeexplore.ieee.org/xpl/abs_free.jsp?isNumber=16678&prod=STD&arnumber=770132&arSt=ared=&arAuthor=&arNumber=770132&a_id0=770132&count=1)  
<http://www.opengroup.org/austin>

**Table 4.3-6: OS Management Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Veritas</a>	Backup Exec	Backup Utility	x86 servers, Novell, MS Windows NT	ALL
<a href="#">American Power Conversion</a>	Powerchute	Interface to UPS	x86 servers, Solaris 7, MS Windows NT, 2000	ALL

**Table 4.3-7: OS Management Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">American Power Conversion</a>	Powerchute	Interface to UPS	x86-based servers, Linux	ALL

**Table 4.3-8: OS Management Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Computer Associates (CA)	ARCserve	Backup Utility	X86 Linux, MS Windows	ALL
IBM Tivoli	Tivoli Storage Manager	Backup Utility	x86 Linux, MS Windows, Solaris, Mainframe	AO

#### 4.3.4 Operating System Security

Operating system-level security mechanisms ensure the integrity of the operating systems through mechanisms such as authentication, authorization, and detection of attacks (e.g. viruses and intrusion). Security must be provided at different levels based on the type of threat considered. Users normally must be authenticated to the operating system before any services are rendered. If there are situations where a guest account is needed, then the services for that account must be well defined and limited in scope. The operating system cannot rely on user authentication alone. Proper configuration of security levels and their periodic review is critical.

Security standard requirements may be satisfied through management policy or through technical features. For example, OS patches should be applied on time, and host-based intrusion detection software should be applied on sensitive / critical systems.

Refer to the Security Services, Section 4.16, for more information about security mechanisms.

##### *Required Standards:*

- Federal Information Processing Standards Publications (FIPS PUBS)  
<http://www.itl.nist.gov/fibspubs/>
- [FIPSPUB140-2](#) SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, 2001 May 25  
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

- FIPS PUB 190 Federal Information Processing Standards Publication 190 1994  
September 28 Announcing the Standard for GUIDELINE FOR THE USE OF  
ADVANCED AUTHENTICATION TECHNOLOGY ALTERNATIVES  
<http://www.itl.nist.gov/fipspubs/fip190.htm>
- FIPS PUB 191 Federal Information Processing Standards Publication 191 1994  
November 9 Announcing the Standard for GUIDELINE FOR THE ANALYSIS OF  
LOCAL AREA NETWORK SECURITY  
<http://www.itl.nist.gov/fipspubs/fip191.htm>  
<http://www.itl.nist.gov/fipspubs/index.htm>

**Table 4.3-9: OS Security Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Tripwire</a>	Tripwire Software	Monitor changes in critical files	x86-based server, MS Windows 2000, Unix	ALL

**Table 4.3-10: OS Security Preferred Products for the Judiciary:**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Tripwire</a>	Tripwire Software	Monitor changes in critical files	x86-based server, Linux	ALL
TBD	Firewall	OS-independent firewall	x86-based workstation	ALL

## 4.4 Software Engineering Services

### 4.4.1 Overview

The production and implementation of portable, scalable, interoperable software is the objective of open systems. Software engineering services provide the infrastructure to develop, maintain, and implement software that exhibits these required characteristics. Software engineering services define the environment for system development.

Architectural models are the method for developing, managing, and implementing new and changed IT applications and infrastructure. Design models model the data, applications, and technology required to support the emerging business needs. Modeling can include diagrams, specifications, and technical drawings to aid in understanding data structures, applications, and supporting technologies.

Software engineering services include the following:

- System Development Methodology
- Business Process Re-engineering
- Data Modeling
- System Development Tools
- System Development Life Cycle (SDLC)

#### 4.4.2 System Development Methodology

Refer to Information Resources Management –IRMS 407.0 –Applications Software Specifications at the following link:

[http://jnet.ao.dcn/Information\\_Technology/IRM\\_Standards/IRMS\\_407.0.html](http://jnet.ao.dcn/Information_Technology/IRM_Standards/IRMS_407.0.html)

#### 4.4.3 Business Process Re-engineering

Business process reengineering (BPR) should precede the design and development or procurement of application software whenever practical. Business Process Reengineering (BPR) accounts for fundamental rethinking and redesign of business processes to achieve dramatic improvements in critical performance measures such as cost, quality, service, and speed. BPR relies on techniques such as Total Quality Management (TQM) and continuous process improvements to achieve desired solutions and project objectives. Critically examining an organization's business practices and changing its fundamental approach by making the business processes simpler and more efficient is a primary goal of BPR.

Business Modeling tools use common definitions and diagrams to facilitate understanding of business functions, information inputs, processes, and products. Examples of business models include the following:

- Business Objects – List of objects (or things, or assets) significant to the organization at a fairly high level of aggregation. The model defines the scope, or boundaries of the objects.
- Semantic Model – Model of the actual enterprise objects (i.e., things, assets) that are significant to the organization. Typically, the semantic model is represented as an entity/relationship model and is at a definition level where concepts expressed (i.e., terms and facts) are those used in significant business objectives/strategies that would later be implemented as business rules.
- Business Processes – List of processes or functions that the organization performs, or the transformation of organization inputs into outputs.
- Business Locations – List of locations in which the organization operates.
- Activity Model (also called a Business Process Model) – Describes the applicable functions associated with the enterprise's business activities, the data and/or information exchanged between activities (internal exchanges), and the data and/or information exchanged with other activities that are outside the scope of the model (external exchanges). Activity Models are hierarchical in nature. They begin with a single box that represents the overall activity and proceed successively to decompose the activity to the level required for the architecture.

The Activity Model captures the activities performed in a business process or mission and the Inputs, Controls, Outputs, and Mechanisms (ICOMs) of those activities. Mechanisms are the resources that are involved in the performance of an activity. Controls, such as legislation or a business rule, represent constraints on an activity. The ICOMS are called activity constraints because each in some way constrains the business processes being modeled.

The Activity Model can be annotated with explicit statements of business rules, which represent relationships among the ICOMs. For example, a business rule can specify who can do what under specified conditions, the combination of inputs and controls needed, and the resulting outputs.

The Activity Model identifies the domain of the model and the viewpoint reflected by the model. Textual descriptions of activity definitions and business flows should be provided, as needed. Annotations to the model may identify the nodes (business locations) where the activities take place or the costs (actual or estimated) associated with performing each activity.

Activity Models should be represented in Unified Modeling Language (UML), a standard modeling language adopted by the Object Management Group (OMG) to support object-oriented analysis, design, and development.

*Referenced Standards:*

- International Organization for Standardization (ISO) OMG UML <http://www.uml.org>
- IEEE/EIA 12207.0-1996/Amd1:2002 Industry Implementation of International Standard ISO/IEC: ISO/IEC12207 Standard for Information Technology Software life cycle processes  
[http://standards.ieee.org/reading/ieee/std\\_public/description/se/12207\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html)

**Table 4.4-1: BPR Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">IBM</a>	Rational Suite Analyst Studio V. 2002.5	UML-based Visual Modeling Tool	x86-based workstation, Microsoft Windows 2000, XP	AO
Troux	Metis	Enterprise Architecture Artifact Manager	x86-based workstation, Microsoft Windows 2000, XP	AO

**Table 4.4-2: BPR Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Business modeling solution		ALL

**4.4.4 Data Modeling**

Data modeling is a business and technical tool that encompasses a set of techniques for analyzing business requirements and designing information system components to manage associated data needs. The purpose of data modeling is to develop an accurate model, or graphical representation, of the user’s information needs and business processes. The data model acts as a framework for the development of the new or enhanced application. Data modeling encourages both the developer and the user to explore the essence or purpose of the application. The data model analysis determines what needs to feed into and what feeds from the core purpose.

Therefore, a data model is any method of visualizing the informational needs of a system and typically takes the form of an Entity Relationship Diagram (ERD).

There are almost as many methods of data modeling, as there are application development methodologies. Data modeling includes analysis and creation of a *database*, *schema*, *table*, *key*, *index*, *relationship*, *columns*, *constraint*, and *trigger*.

- The *schema* is the structure of a database system, describing the data model to be used for retrieval and storage of data. In a relational database, the schema defines the tables, the fields in each table, and the relationship between the fields and tables. The schema is the biggest unit that can be worked with at any given time.
- An *index* is a physical data structure that supports faster access to records in a table. Indexes are constructed from one or more columns from a single table. Since indexes only enhance performance of access they are not defined in the logically data model.
- A *table* is the basic modeling structure of a relational database. It represents a set of records of the same structure, also called rows. Each of these records contains data. The information about the structure of a table is stored in the database itself.
- *Keys* are used to access the table. Primary keys uniquely identify a row in a table, while foreign keys access data in other related tables.
- A *relationship* is a dependency of any kind between tables in a data model. A relationship is a summary of a stereotyped association and a set of primary and foreign keys. Every relationship is between a parent and child table, where a parent table must have a primary key defined. The child table creates a foreign key column and foreign key constraint to address the parent table. A non-identifying association represents a relationship between two independent tables. The foreign key of the child table does not contain all of the primary key columns.
- A table contains *columns* that are tagged attributes. Columns can contain data, when they are instantiated as a row. A column must have a defined data type. The column can be either persistent or computed.
- A *constraint* is a rule applied to the structure of the database. This rule extends the structure and can be applied to a column and/or table. All constraints are defined as stereotyped operations. The primary key constraint defines the primary key as a rule on the table. The foreign key constraint defines the foreign key as a rule on the table.
- A *trigger* is a special form of stored procedures that goes into effect when you insert, delete, or update a specified table or column. You can use triggers to enforce referential integrity. Referential integrity triggers exist for certain databases, such as Informix.

Data modeling tools include object-relational mapping, database schema generation and modification from system development object models, and roundtrip engineering between models and database management systems. They control changes to the models, record and report changes, and verify compliance with specified requirements.

Examples of data models include:

- Logical Data Model – Refers to the user’s view of the way data is organized. The logical data model represents the objects of the organization about which it records information, in either automated or non-automated form. It is represented as a fully attributed, keyed, normalized entity relationship model reflecting the intent of the semantic model (reference Business Process Reengineering, Section 4.4.3).
- Class Model – Similar to a logical data model; describes static information and relationships between information. A class model also describes informational behaviors. The class model can be used to model various levels of granularity.
- Physical Data Model – Refers to the actual organization of data in a technology constrained, or physical representation of the objects of the enterprise. The representation style of this model depends on the technology chosen for implementation. If relational technology is chosen, this is a model of the table structure required to support the logical data model in a relational-style model. In an object-oriented notation, this is a class-hierarchy/association style model.
- Data Definition “Library or Encyclopedia” – Definition of all the data objects specified by the physical data model; includes all the data definition language required for implementation.
- Sequencing Plan – Outline of the uninterrupted flow and management of data, its use by both legacy and new systems, and its creation and distribution. Used to ensure data migration is managed and pursued incrementally so that the impact of unforeseen events, (e.g., technical problems, fiscal delays, etc.) on business unit operations is minimized.

*Referenced Standards:*

- IEEE/EIA 12207.0-1996 Industry Implementation of International Standard ISO/IEC: ISO/IEC12207.0-1996/Amd1:2002 Standard for Information Technology Software Life Cycle Processes  
[http://standards.ieee.org/reading/ieee/std\\_public/description/se/12207\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html)

**Table 4.4-3: Data Modeling Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">IBM</a>	Rational Suite Analyst Studio V. 2002.5	Data modeling solution	x86-based workstation, Microsoft Windows 2000, XP	AO
CA	ERwin Data Modeler	Data modeling	x86-based workstation, Microsoft Windows 2000, XP	AO

**Table 4.4-4: Data Modeling Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data modeling solution		

#### 4.4.5 System Development Tools

System development tools are required to develop, maintain, and/or implement automated information systems (AISs). A standard toolset leverages the experience of in-house staff to work on different projects without retraining on system development tools and procedures.

Most of the Judiciary applications are commercial software implementations. Conformance to the Judiciary Enterprise Architecture is a prime criterion for selection of commercial software application. If the commercial software application has a choice of subcomponents (i.e. databases, report writers, etc) then select those components that fit within the Enterprise Architecture. If this is not possible then a waiver is required.

*Required Standards:*

- Software Engineering Institute Capability Maturity Model reference <http://www.sei.cmu.edu/cmm/cmms/transition.html>
- IEEE Std 1362-1998 (Incorporates IEEE Std 1362a-1998) IEEE Guide for Information Technology -- System Definition -- Concept of Operations (ConOps) Document [http://standards.ieee.org/reading/ieee/std\\_public/description/se/1362-1998\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/1362-1998_desc.html)
- IEEE STD 1016-1998 IEEE Guide to Software Design Descriptions [http://standards.ieee.org/reading/ieee/std\\_public/description/se/1016-1998\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/1016-1998_desc.html)
- IEEE/EIA 12207.0-1996/Amd1:2002 Industry Implementation of International Standard ISO/IEC: ISO/IEC12207 Standard for Information Technology Software life cycle processes [http://standards.ieee.org/reading/ieee/std\\_public/description/se/12207\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html)
- IEEE Std 2001-1999, IEEE Recommended Practice for Internet Practices – Web Page Engineering – Intranet/Extranet Applications, May 1 <http://dx.doi.org/10.1041/standard/2001>
- Java 2 Platform Enterprise Edition (J2EE) standards (Refer to <http://java.sun.com/j2ee/docs.html> and <http://java.sun.com/j2ee/faq.html>)

##### 4.4.5.1 Primary System Development Tools

Client-server applications are typically two-tier applications deployed on a private network where: 1) a client program establishes connections for the purpose of sending requests, and 2) a server program accepts connections in order to service requests by sending back responses. Any given program may be capable of being both a client and a server; the terms refer to the role being performed by the program for a particular connection, rather than to the program's capabilities in general.

**Table 4.4-5: System Development Tool Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Crystal Decisions</a>	Crystal Reports 8.0, 9.0	Report Writer	x86-based workstation, MS Windows 95, 98, ME, ME, NT, 2000, XP	
<a href="#">Hyperion</a>	SQR Server 6.0	Report Writer	x86-based server, Solaris 7	FAS <sup>1</sup>
<a href="#">IBM</a>	Lotus Notes Designer	Notes Application Development	x86-based workstation, MS Windows 95, 98, ME, ME, NT, 2000, XP	AO
Adobe	LiveCycle Suite	Form Development Workflow	x86-based workstation, MS Windows 95, 98, ME, ME, NT, 2000, XP, Linux servers	ALL

**Table 4.4-6: System Development Tool Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Eclipse Foundation	Eclipse	Integrated Development Environment (IDE)	x86-based workstation	ALL
Business Objects	Enterprise Reports Server	Business Intelligence	X86-based servers, Linux	ALL
Business Objects	Crystal Reports Server	Report Writer	X86-based servers, Linux	ALL
Business Objects	Crystal Reports Developer, Professional, and Standard Edition	Report Writer	X86-based workstation, Microsoft Windows 2000, XP	ALL

#### 4.4.5.2 Web Application Development

Web application development generally utilizes a multi-tier architecture. The tiers include: a Presentation Layer, which manages the user interface; a Business Logic Layer, which executes application functions that deal with business logic and flow control; and a Data Access layer, which executes the logic relating to data storage and retrieval<sup>2</sup>. One or more components may be used to implement each tier.

##### *Required Standards:*

- Network Information Center (NIC) Request for Comment (RFC) – 2616 Hypertext Transfer Protocol  
<http://www.rfc-editor.org/rfc/rfc2616.txt>  
<http://www.w3.org/Protocols/> for W3C standards on HTTP 1.0 and HTTP 1.1
- ANSINCITS 331.1-1999 Technology - SQLJ - Part 1: SQL Routines Using the Java Programming Language
- ANSINCITS 331.2-2000 Information Technology - SQLJ - Part 2: SQL Types Using the Java™ Programming Language

<sup>1</sup> FAS: FAS4T waiver

<sup>2</sup> The architecture is described in detail in the section on Distributed Computing Services.

**Table 4.4-7: Web Application Development Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Adobe</a>	Acrobat 4.0, 5.0, 6.0, 7.0, 8.0	PDF generator, reader, and editing tool	x86-based workstation, Windows 95, 98, ME, ME, NT, 2000, XP	ALL
<a href="#">Microsoft</a>	Visual Studio 6.0	Microsoft Visual Basic 6.0, Visual C++ 6.0, Visual J++ 6.0, or Visual FoxPro 6.0. Visual InterDev 6.0	x86-based workstation, Windows 95, 98, ME, ME, NT, 2000, XP	AO
<a href="#">Microsoft</a>	Visual Basic 6	Supports the Component Object Model (COM), Distributed COM (DCOM)	x86-based workstation, Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Visual FoxPro	Supports the Component Object Model (COM), Distributed COM (DCOM)	x86-based workstation, Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Sun</a>	J2EE	Java Enterprise Edition	x86-based servers, Solaris	ALL

**Table 4.4-8: Web Application Development Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Adobe</a>	Acrobat 7.0	PDF generator	x86-based workstation, MS Windows 2000, XP	ALL
<a href="#">Peoplesoft</a>	Peopletools 8.4	Integrated Development Environment to develop Web applications for commercial PeopleSoft	x86-based workstation, Linux, Microsoft Windows 2000, XP	HRM <sup>1</sup>

**Table 4.4-9: Web Application Development Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Sun</a>	J2EE	Java Enterprise Edition	x86-based servers, Linux	ALL
<a href="#">Eclipse</a>	Eclipse	Integrated Development Environment	x86-based workstation, Linux, Microsoft Windows 2000, XP	ALL

<sup>1</sup> Used by Human Resources, not entire judiciary

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Macromedia</a>	Dreamweaver	Manage Web Content	x86-based workstation, MS Windows 95, 98, ME, ME, NT, 2000, XP	AO
<a href="#">Macromedia</a>	ColdFusion	Manage Web Content	x86-based server, MS Windows NT, 2000	AO

#### 4.4.5.3 Web Authoring Tools

Web authoring tools are a special subset of Web Development tools used to develop, create, or mark up documents for importing to Internet Web pages. The products can be used to create unique Web pages from scratch or convert documents or files from applications such as Microsoft Word, PowerPoint, or WordPerfect into innovative Web pages. Hypertext Markup Language (HTML) is the *lingua franca*, or common language, for publishing hypertext on the World Wide Web. It is a non-proprietary format based upon Standard Generalized Markup Language (SGML), and can be created and processed by a wide range of tools, from simple plain text editors—where text is typed in—to sophisticated “What You See is What You Get” (WYSIWYG) authoring tools. HTML uses tags such as <h1> and </h1> to structure text into headings, paragraphs, lists, hypertext links, etc.

The Extensible HyperText Markup Language (XHTML) is a family of current and future document types and modules that reproduce, subset, and extend HTML, reformulated in Extensible Markup Language (XML). XHTML Family document types are all XML-based, and ultimately are designed to work in conjunction with XML-based user agents. XHTML is the successor of HTML, and a [series of specifications](#) has been developed for XHTML.

##### *Required Standards:*

- Hypertext Markup Language (HTML), subset of SGML, ANSI/ISO 8879:1986<sup>1</sup>
- Extensible HyperText Markup Language (XHTML) <http://www.w3c.org/TR/xhtml1/><sup>2</sup>
- Standard Generalized Markup Language (SGML), ANSI/ISO 8879:1986
- Extensible Markup Language (XML) 1.1 (Third Edition), 2004

##### *Standards Overview:*

For further information refer to

- W3C Recommendation for HTML 4.01 Specification: <http://www.w3c.org/TR/html/>
- W3C Overview of SGML Resources: <http://www.w3c.org/MarkUp/SGML>

**Table 4.4-10: Web Authoring Tool Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Microsoft</a>	FrontPage	Web Page Generation	x86-based workstations, MS Windows	

<sup>1</sup> For SGML standards refer to Data Interchange Services.

<sup>2</sup> XHTML – refer to Section 4.7.4.4

Vendor	Product	Function	Judiciary Platform	Scope
Adobe <a href="#">Macromedia</a>	ColdFusion	Web Application Builder	x86-based servers, MS Windows NT, 2000	

**Table 4.4-11: Web Authoring Tool Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Open Source	PHP	Web Authoring Environment	X86 platforms (server and workstation)	ALL

#### 4.4.5.4 Traditional Programming Languages

Traditional programming languages provide the capability to facilitate various levels of programming from low-level (hardware control) operations to high-level abstract functions and procedures.

*Required Standards:*

- ANSI/ISO 9899:1992 - C
- ANSI/ISO/IEC 9899-1999 – Programming Languages – C (revision of ANSI/ISO 9899-1990 (R1997)). <http://www.nssn.org/>
- Java and its associated specifications:  
The Java language specification. <http://java.sun.com/docs/books/jls/>  
The Java virtual machine specification, <http://java.sun.com/docs/books/vmspec/>

**Table 4.4-12: Programming Language Products Used by the Judiciary**

Vendor	Programming Language	Scope
Open Source and Proprietary	C / C++	ALL
<a href="#">Microsoft</a>	Visual Basic 6.0	AO
Open Source	Perl5	ALL
<a href="#">Sun Microsystems</a>	Java	ALL
<a href="#">IBM</a>	VS Fortran	AO <sup>1</sup>
<a href="#">IBM</a>	OS/VS COBOL	AO
<a href="#">IBM</a>	VS COBOL	AO

**Table 4.4-13: Programming Language Preferred Products for the Judiciary**

Vendor	Programming Language	Scope
Open Source	Perl5	ALL
Open Source and Proprietary	C/C++	ALL
<a href="#">Sun Microsystems</a>	Java (J2SE, J2EE, J2ME)	ALL
<a href="#">IBM</a>	VS Fortran	AO <sup>1</sup>

<sup>1</sup> Used by the AO Mainframe

Vendor	Programming Language	Scope
<a href="#">IBM</a>	OS/VS COBOL	AO
<a href="#">IBM</a>	VS COBOL	AO

#### 4.4.5.5 Web Application Development Language

Programming languages, such as Java, are the foundation for scalable component framework-based multi-tier Internet and/or Intranet-oriented application development.

*Required Standards:*

- Java by Sun Microsystems, Inc.
  - JavaServer Pages™ Specification, <http://Java.sun.com/products/jsp/download.html>
  - Java™ Servlet Specification, <http://Java.sun.com/products/servlet/download.html>
  - Java™ 2 SDK, Enterprise Edition Specification, v 1.4  
<http://java.sun.com/j2ee/1.4/download-sdk.html>
  - Enterprise JavaBeans™ Specification, <http://Java.sun.com/products/ejb/docs.html>
  - Java™ 2 Platform, standard Edition specification, <http://java.sun.com/j2se/>
  - Java™ 2 Platform, Micro Edition specification <http://java.sun.com/j2me/docs/>
  - The Java language specification, <http://java.sun.com/docs/books/jls/>
  - The Java virtual machine specification, <http://java.sun.com/docs/books/vmspec/>
- HTML standard 4.01, [HTML Home Page http://www.w3.org/TR/html/](http://www.w3.org/TR/html/)
- [Extensible Hypertext Markup Language \(XHTML\) 1.1](http://www.w3c.org/MarkUp/), W3C's recommendation for the latest version of HTML, <http://www.w3c.org/MarkUp/> and <http://www.w3c.org/TR/xhtml11>

**Table 4.4-14: Web Application Language Products Used by the Judiciary**

Vendor	Programming Language	Scope
Multiple vendors	HTML/XML/CSS	ALL
<a href="#">Sun Microsystems</a>	Java	ALL
Multiple vendors	JavaScript	ALL
Open source	Perl5	ALL

**Table 4.4-15: Web Application Language Preferred Products for the Judiciary**

Vendor	Programming Language	Scope
<a href="#">Sun Microsystems</a>	<a href="#">Java</a>	ALL
Multiple vendors	HTML/XML/CSS	ALL
Multiple vendors	JavaScript	ALL
Open source	Perl5	ALL

#### 4.4.5.6 Web Application Development Environment

Integrated Development Environments (IDEs) are used for Internet and/or Intranet application development. IDEs provide a suite of software programs / tools which make development easier by introducing a level of abstraction which allows the developer to define programs using English-like scripting language and graphical representation. The IDE generates software based on the parameters entered and metadata describing the application data. The IDE may provide guidance, define constraints, and provide project management functions and/or configuration control. The IDE may integrate development tools with the execution platform.

Required Standards:

- J2EE

**Table 4.4-16: IDE Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Macromedia	Dreamweaver MX	Create Web Applications	x86-based workstation, MS Windows 95, 98, ME, ME, NT, 2000, XP	AO
Macromedia	ColdFusion MX	Create Web Applications	x86-based server, MS Windows NT, 2000	AO

**Table 4.4-17: IDE Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Deployment Platform	Scope
Eclipse Foundation	Eclipse	Generic IDE and rich client	x86-based workstation	ALL

#### 4.4.6 System Development Life Cycle

The system development life cycle (SDLC) process includes methodology and supporting system development tools. A standard methodology supported by a standard toolset reduces maintenance costs, makes system development more predictable, and lessens dependence on the original developers for maintenance.

The IT development manager should consider the size, complexity, and scope of the project and choose the most appropriate tools to satisfy the business need. The Judiciary TRM will list preferred development tools. The majority of Judiciary projects are COTS system implementations. In general, the tasks and work products that apply when the life cycle approach is tailored for a COTS implementation are: (1) a succinct functional requirements statement; (2) consideration and use of Judiciary standard data; (3) operation within the Judiciary's current and planned IT environment, i.e., consistency with the TRM; (4) system integration and system and user-acceptance testing; (5) user training; (6) user and help desk manuals (preferably context-sensitive help is provided within the application); and (7) operations and maintenance manuals.

In the case of custom-developed applications, large commercial software implementations, and initiatives to develop Judiciary-wide enterprise infrastructure systems and shared data

repositories, software development lifecycle products are absolutely essential for successful development and implementation.

#### 4.4.6.1 Project Management

Project management (PM) utilizes automated tools to facilitate and support project management operations, and to track actual against planned schedule, budget, and contract performance. The tools are used to generate critical trend analysis, reports, and the necessary visibility for business and technical managers to identify problems and initiate corrective actions.

*Referenced Standards:*

- IEEE STD 1058-1998 IEEE Standard for Software Project Management Plans  
[http://standards.ieee.org/reading/ieee/std\\_public/description/se/1058-1998\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/1058-1998_desc.html)

**Table 4.4-18: PM Products Used by the Judiciary**

Vendor	Product	Function	Platform	Scope
<a href="#">Microsoft</a>	Project 98 / 2000 / 2002	Project Management	x86-based workstation, Windows 95, 98, ME, ME, NT, 2000, XP	ALL

**Table 4.4-19: Preferred Products for the Judiciary**

Vendor	Product	Function	Platform	Scope
<a href="#">Microsoft</a>	Project 2002?	Project Management	x86-based workstation, Microsoft Windows 2000, XP	ALL

#### 4.4.6.2 Requirements Management

Requirements management (RM) is a formal management discipline to ensure definition, allocation, tracking, and verification of automated information systems functional, data, interface, and performance requirements. A requirement is a condition or capability needed by a user to solve a problem or achieve an objective. Requirements management is used to verify that the requirements to be satisfied by the project are identified, reported, accounted for, and tracked in compliance with established standards and procedures. RM-related tasks include requirements entry or extraction, maintenance, decomposition and allocation to higher/lower-level requirements, design components and test and verification activities, as well as report generation. To facilitate the performance of these tasks, an automated RM tool will be selected.

*Referenced Standards:*

- IEEE STD 830-1998 IEEE Recommended Practice for Software Requirements Specifications  
[http://standards.ieee.org/reading/ieee/std\\_public/description/se/830-1998\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/830-1998_desc.html)
- IEEE STD 1233-1998 IEEE Guide for Developing System Requirements Specifications  
[http://standards.ieee.org/reading/ieee/std\\_public/description/se/1233-1998\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/1233-1998_desc.html)
- System Engineering Institute Capability Maturity Model  
<http://www.sei.cmu.edu/cmm/cmms/transition.html>

**Table 4.4-20: Requirements Management Products Used by the Judiciary**

Vendor	Product	Function	Platform	Scope
<a href="#">IBM</a>	Rational Suite Analyst Studio V 2002.05	Capture, Report, and Trace Requirements	x86-based workstation, Windows 95, 98, ME, ME, NT, 2000, XP	AO

**Table 4.4-21: RM Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.4.6.3 Configuration Management

Configuration Management (CM) is a discipline applying technical and administrative direction and surveillance to:

- Version Management – Tracking and controlling versions of files. Version Management includes capabilities such as labeling, branching, merging, version content comparisons, and security and permission management across version-controlled projects.
- Defect Tracking – The identification, assignment, and management of discovered defects within an application, product, or solution. Defect tracking tools provide searchable defect data to identify urgent and related defects or bugs. The architecture should be built to facilitate the pushing of software patches across the enterprise.
- Issue Management – Management of business, technical, and infrastructure issues throughout the entire lifecycle of a project.
- Task Management – Requirements, testing, and issues assignments are transformed into prioritized tasks. Task Management tools provide automation features for managing, delivering, assigning, reminding, and collaborating task management and execution.
- Change Management – Management of application code and content changes across the software development lifecycles.
- Deployment Management – The capability of software delivery to remote networked desktops, servers, and mobile devices across an enterprise. Deployment automation tools provide centralized and accelerated delivery of applications to users via push technologies, eliminating the need for manual installation and configuration.

A configuration management tool includes a repository to maintain an indexed hierarchical configuration list of project components, associated descriptions and metadata, allocation to design elements, and a centralized change and release management log. Configuration management incorporates automated analyses of dependencies between components. Through knowledge of these dependencies inconsistencies are minimized and adequate performance of CM-controlled builds can be ensured.

In addition, the CM repository must have the ability to manage and maintain multiple versions and baselines to support on-demand retrieval. This feature also supports the Development Manager to perform activities through the development phase of the project. The CM repository also allows other project entities to oversee project status and activities at various phases of the LCM.

*Referenced Standards:*

- IEEE Std 828-1998, IEEE Standard for Software Configuration Management Plans [http://standards.ieee.org/reading/ieee/std\\_public/description/se/828-1998\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/828-1998_desc.html)
- IEEE/EIA 12207.0-1996 Industry Implementation of International Standard ISO/IEC: ISO/IEC12207 Standard for Information Technology Software life cycle processes [http://standards.ieee.org/reading/ieee/std\\_public/description/se/12207\\_desc.html](http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html)
- The Software Engineering Institute at Carnegie-Mellon University <http://www.sei.cmu.edu/cmm/cmms/transition.html>

**Table 4.4-22: CM Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Open Source	Source Code Control System (SCCS)	Configuration Management	Sun Solaris, Linux	ALL
<a href="#">IBM</a>	Rational Suite Analyst Studio V 2002.05	Configuration Management	x86-based workstation, Windows 95, 98, ME, ME, NT, 2000, XP	AO
Microsoft	Visual Source Safe V 6.0	Configuration Management	x86-based workstation, Windows 95, 98, ME, ME, NT, 2000, XP	AO
Open Source	RCS	Configuration Management	Solaris	ECF

**Table 4.4-23: CM Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Open Source	Concurrent Versions System (CVS)	Configuration Management	x86-based workstation and servers	ALL

**Table 4.4-24: CM Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Open source	CVS	Configuration Management	Linux	ALL

**4.4.6.4 Test Management**

Test Management (TM) activities include test planning, designing (test cases), execution, reporting, code coverage, and harness development.

- *Functional Testing* – Testing that focus on any requirements that can be traced directly to use cases (or business functions), business rules, and design.
- *Business Cycle Testing* – The emulation of activities performed over a period of time that is relevant to the application under test.
- *Usability Testing* – Testing to ensure that the application navigation, functionality, and graphical user interface (GUI) allow a user to effectively and efficiently do their work in a way that they are satisfied with the application.
- *Section 508 Testing (If applicable)* – Testing to ensure that the software is usable by users with disabilities.
- *Performance Profiling* – Performance testing that measures and evaluates response times and transaction rates.
- *Load/Stress/Volume Testing* – Testing that measure and evaluate how a system performs and functions under varying workloads, large amounts of data and/or resource utilization.
- *Security and Access Control Testing* – Focusing on the technical, administrative, and physical security controls that have been designed into the system architecture in order to provide confidentiality, integrity, and availability.
- *Reliability Testing* – Tests to verify that failover methods are invoked properly and the system recovers properly.
- *Configuration Testing* – Tests to ensure that the application or system can handle all hardware and software variables and requirements that have been defined.
- *Installation Testing* – Refers to the verification that the software installation process works properly in different environments and among varying conditions.

#### **4.5 Human Computer Interface Services**

Human Computer Interface Services describe the following areas:

- Traditional User Interface
- Web Graphical User Interface
- Alternate User Interface
- Multimedia Interface
- Terminal Emulation

##### **4.5.1 Traditional Graphical User Interface**

A standard GUI is used to provide users with an intuitive and user-friendly working computer environment. The GUI defines how the user interacts with the system. It also controls the screen appearance. The GUI should offer users easy access to computer functions. It should allow a user to enter commands into a system through the use of menus or by pointing to icons rather than typing command sequences on the keyboard.

*Required Standards:*

- Industry standards used in Visual Interdev, Visual Basic and Visual C++ by Microsoft Corporation
- *The Windows Interface Guidelines for Software Design*

**Table 4.5-1: GUI Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Borland</a>	Jbuilder Studio	GUI design	x86-based workstation, MS Windows 95, 98, ME, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Visual Basic 6.0	GUI design	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Visual C++ 6.0	GUI design	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Visual FoxPro 7.0	GUI design	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Visual Access 2002	GUI design	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Symantec</a>	Visual Café	GUI design	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Sybase</a>	PowerBuilder 6.5, 7.0	GUI design	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	

**Table 4.5-2: GUI Preferred Product for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD			x86-based workstation	

## 4.5.2 Web Graphical User Interface

The Web Graphical User Interface consists of two logical components, which interoperate using the request/response Hypertext Transfer Protocol (HTTP)<sup>1</sup>.

*Required Standards:*

- RFC 2616 HyperText Transfer Protocol  
<http://www.rfc-editor.org/rfc/rfc2616.txt>  
<http://www.w3c.org/Protocols/> for W3C standards on HTTP 1.0 and HTTP 1.1
- HTML standard 4.01, [HTML Home Page http://www.w3c.org/TR/REC-html40/](http://www.w3c.org/TR/REC-html40/)
- [Extensible Hypertext Markup Language \(XHTML\) 1.1](http://www.w3c.org/TR/2001/REC-xhtml11-20010531/), W3C's recommendation for the latest version of HTML, <http://www.w3c.org/MarkUp/> and <http://www.w3c.org/TR/2001/REC-xhtml11-20010531/>

<sup>1</sup> HTTP is described in more detail in Section 4.15.8, Communication Protocols.

- W3C REC-CSS1-19900111, Cascading Style Sheets, Level 1, W3C Recommendation 17 December 1996, revised 11 January 1999, <http://www.w3c.org/TR/1999/REC-CSS1-19990111>
- W3C REC-CSS1-20040225, Cascading Style Sheets, Level 21, Requires 1, W3C Recommendation <http://www.w3c.org/TR/CSS21>

#### 4.5.2.1 Web Browser

A web browser is a client program that uses the Hypertext Transfer Protocol (HTTP) to make requests to web servers through the Internet on behalf of the browser's users. Browsers are required to provide client interconnection services to access global or public networks such as the Internet and for Intranet or Extranet.

**Table 4.5-3: Web Browser Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Netscape</a>	Netscape Communicator / Navigator, various versions	Web browser provides client interconnection services to access Judiciary or public networks.	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Internet Explorer, various versions	Web browser provides client interconnection services to access Judiciary or public networks.	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
Mozilla	Firefox	Web browser provides client interconnection services to access Judiciary or public networks.	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP x86-based server	

**Table 4.5-4: Web Browser Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Microsoft</a>	Internet Explorer 6.x, 128 bit encryption	Web browser provides client interconnection services to access Judiciary or public networks.	x86-based workstation, MS Windows 2000, XP	
<a href="#">Netscape</a>	Netscape Communicator 7.x, 128 bit encryption	Web browser provides client interconnection services to access Judiciary or public networks.	x86-based workstation, Linux, MS Windows 2000, XP; x86-based servers, Linux	

Vendor	Product	Function	Judiciary Platform	Scope
Mozilla	Firefox 2.0	Web browser provides client interconnection services to access Judiciary or public networks.	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP, Linux x86-based server, Linux	

#### 4.5.2.2 Web Server<sup>1</sup>

A web server is a server which responds to Hypertext Transfer Protocol (HTTP) requests, and is configured and optimized to deliver Hypertext Markup Language (HTML) pages using HTTP. The responsibility of the server is to implement core HTTP protocol features. A content generator is a means by which requests are mapped to content, which is optionally transformed, generated or otherwise prepared, and then passed back to the server, which then sends it to the client. The generator may be, but is not necessarily, external to the server.

*Required Standards:*

- HTTP/1.0 and 1.1 (RFC1945 and 2616)  
RFC 1945, <http://www.rfc-editor.org/rfc/rfc1945.txt>  
RFC 2616, <http://www.rfc-editor.org/rfc/rfc2616.txt>

For the latest information on W3C standards on HTTP protocol, refer to <http://www.w3c.org/Protocols/>

- DOM (Document Object Model) Level 1, <http://www.w3c.org/TR/REC-DOM-Level-1/>  
DOM Level 2, <http://www.w3c.org/TR/DOM-Level-2/>
- W3C HTML home page, <http://www.w3c.org/MarkUp/>
- HTML 4.01 Specification, W3C Recommendation 24 December 1999, <http://www.w3c.org/TR/html4/>
- XHTML 1.0, XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition), A Reformulation of HTML 4 in XML 1.0, W3C Recommendation 26 January 2000, revised 1 August 2002 <http://www.w3c.org/TR/xhtml1/>
- XHTML 1.1, Module-based XHTML, W3C Recommendation 31 May 2001, <http://www.w3c.org/TR/xhtml11/>
- XML (Extensible Markup Language) 1.0, <http://www.w3c.org/XML/>
- XML schema, W3C recommendation, May 2001, [XML Schema Part 0: Primer](http://www.w3c.org/TR/xmlschema-0/), [XML Schema Part 1: Structures](http://www.w3c.org/TR/xmlschema-1/) <http://www.w3c.org/TR/xmlschema-1/>  
[XML Schema Part 2: Datatypes](http://www.w3c.org/TR/xmlschema-2/) <http://www.w3c.org/TR/xmlschema-2/>
- RFC 1157, SNMP (Simple Network Management Protocol), <http://www.rfc-editor.org/rfc/rfc1157.txt>
- The Resource Description Framework (RDF) integrates a variety of web-based metadata activities including sitemaps, content ratings, stream channel definitions, search engine data collection (web crawling), digital library collections, and distributed authoring, using XML as interchange syntax. (<http://www.w3c.org/RDF/>).

<sup>1</sup> Web Servers: Perspectives, Gartner Group, January 11, 2000

**Table 4.5-5: Web Server Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Apache Software foundation</a>	Apache 1.x, 2x	Intra/internet Web Server A reference implementation of the HTTP protocol	x86-based servers, Sun Solaris 7, Linux	ALL
<a href="#">Apache Software foundation</a>	Jakarta Tomcat	Java-Based Web Server	x86-based servers, Sun Solaris 7	
<a href="#">Macromedia</a>	ColdFusion Server 5, MX	Web/web application server	x86-based server, Microsoft Windows NT, 2000	
<a href="#">Microsoft</a>	Internet Information Server (IIS) 4.0, 5.0, MX	Intra/internet Web Server	x86-based server, Microsoft Windows NT, 2000	AO
<a href="#">BEA</a>	WebLogic 6.1	Web application server (Used bundled with commercial applications)	x86-based servers, Sun Solaris 7	FAS <sup>1</sup>
IBM	WebSphere	Web Applications Server	Space-based Series	MJ

**Table 4.5-6: Web Server Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Apache Software foundation</a>	Apache 2x	Intra/internet Web Server A reference implementation of the HTTP protocol	x86-based servers, Linux	ALL
<a href="#">BEA Systems</a>	WebLogic	Web application server (used bundled with commercial applications)	x86-based servers, Linux	FAS <sup>1</sup>

### 4.5.3 Alternate User Interface

The alternate user interface includes the software products or mechanisms used for alternate target human interface devices such as handheld devices (personal digital assistants) and the development or enhancement of human interface mechanisms for those with disabilities such as visual and hearing impairments.

Although the Judiciary is not required to be compliant with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), the Judiciary intends to meet the spirit of the law. Under Section 508, federal agencies that develop, procure, maintain, or use electronic and information

<sup>1</sup> FAS: FAS4T waiver

technology, must give disabled employees and members of the public access to information that is comparable to the access available to others, unless an undue burden would be imposed on the agency.

Subpart A (General) of the 508 standard defines the types of technology covered and sets forth provisions that establish a minimum level of accessibility. They cover the full range of electronic and information technologies in the federal sector, including those used in communication, duplication, computing, storage, presentation, control, transport, and production. This includes computers, software, networks, peripherals, and other types of electronic office equipment. Information technology is defined, in part, as “any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information.” The standards also cover technology procured by federal agencies under contract with a private entity, but apply only to those products directly relevant to the contract and its deliverables. For example, if an agency contracts with a firm to develop its web site, the standards would apply to the new web site for the agency, but not to the firm’s own web site.

Subpart B (Technical Standards) provides technical specifications and performance-based requirements, which focus on the functional capabilities of covered technologies. In particular, the following technologies are covered: Software Applications and Operating Systems; Web-based Intranet and Internet Information and Applications; Telecommunications Products; Video or Multimedia Products; Self-contained, Closed Products; and Desktop and Portable Computers. Functional Performance Criteria and Information, Documentation, and Support are covered under Subparts C and D.

Compliance with Section 508 requirements is more of an implementation issue than a product issue for programmers and developers. For example, it is meaningless to say that Java or C++ are, or are not, 508 compliant, as both can be used to support the development and implementation of compliant systems. A majority of the Judiciary’s systems are COTS products. Since COTS system’s vendors are usually responsible for including 508-compliance functionality, they should be asked to prove compliance prior to purchase.

For individual products, a copy of an independent assessment that indicates compliance with the Access for Final Accessibility Standards for Electronic and Information Technology covered by Section 508 should be requested from the vendor. When dealing with custom-developed systems, making a product compliant is much easier if it is designed into the product rather than leaving to the end and attempting a retrofit.

*Required Standards:*

- Web Content Accessibility Guidelines 1.0, W3C Organization, <http://www.w3c.org/TR/WAI-WEBCONTENT>, 1999
- Section 508 Standards, <http://www.section508.gov/>

**Table 4.5-7: Alternate User Interface Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.5-8: Alternate User Interface Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**Table 4.5-9: Alternate User Interface Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Freedom Scientific</a>	JAWS for Windows 5.0	Screen reader	x86-based workstation, MS Windows 2000, XP	
<a href="#">Freedom Scientific</a>	MAGic 8.02	Screen Magnifier	x86-based workstation, MS Windows 2000, XP	AO

#### 4.5.4 Multimedia Interface

Although still images and text can be described as multimedia in a broad sense, multimedia is typically used to mean the combination of text, sound, and/or motion video and can mean any of the following:

- Text and sound
- Text, sound, and still or animated graphic images
- Text, sound, and video images
- Video and sound
- Multiple display areas, images, or presentations presented concurrently

Multimedia is distinguished from traditional motion pictures or movies both by the scale of the production (multimedia is usually smaller and less expensive) and by the possibility of audience interactivity and involvement. Multimedia can allow users any of the following: voice command, mouse manipulation, text entry, touch screen, video capture of the user, or live participation (in live presentations). Multimedia tends to be more sophisticated (and relatively more expensive) than simple text-and-images. Movies (digitized or not), pure images, and text are often considered part of multimedia.

Multimedia interface is possible in many contexts, including the Web, CD-ROMs, and live theater. For CD-ROMs, a multimedia software player is needed to render its content; for the Web, there can be an additional and optional streaming server for delivering multimedia content in an efficient and convenient way.

Popular multimedia players include Quicktime from Apple, Shockwave from Micromedia, Media Player from Microsoft, and RealOne Player from RealNetworks. These players are software applications that decode digitized media content and render it appropriately. Streaming servers deliver a sequence of content that are sent in compressed form over the Internet and displayed by the player as they arrive. With streaming video or streaming audio, a Web user does not have to wait to download a large file before seeing the video or hearing the sound. Major

streaming servers include Helix Universal Server from RealNetwork, Microsoft Windows Media Technologies (including its NetShow Services and Theater Server).

**Table 4.5-10: Multimedia Interface Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Apple Computer Inc.</a>	Quick Time Player	Mpeg movie view	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Macromedia</a>	Director MX	Audio/video editor and player	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Windows Media Player	Audio / video player	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Real Networks</a>	Real Player	Audio/video player	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	

**Table 4.5-11: Multimedia Interface Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.5.5 Terminal Emulation

Terminal emulation refers to thin-client remote access to computers across local and wide-area networks (WANs). Client software is used to connect to a host running terminal emulation services. All computing takes place on the host computer. Screen updates are transmitted from the host to the client. The client software may be embedded within a dedicated appliance (such as early mainframe terminals) or may be installed on a workstation or other multi-function device. There are several types of terminal emulation services including IBM's TN-3270 standard for connection to mainframes, Novell's RConsole, and Microsoft's Terminal Services for Windows.

**Table 4.5-12: Terminal Emulation Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Microsoft</a>	Windows NT 4.0 Terminal Server Edition	Terminal Server services	x86-based server, Microsoft Windows NT 4.0 Terminal Server Edition	
<a href="#">Microsoft</a>	Windows 2000	Terminal Server services	x86-based server, Microsoft Windows 2000	

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Citrix</a>	Metaframe	Terminal server supports cross-platform access; integration tool that emulates embedded objects, security and management capabilities	x86-based server, Microsoft Windows NT 4.0 Terminal Server Edition, Windows 2000	
<a href="#">Hummingbird</a>	Exceed	Terminal Emulator Exceed permits applications, normally available only on UNIX workstations, to be readily accessed by Windows workstations	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">PuTTY</a>	PuTTY	SSH Client	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	ALL

**Table 4.5-13: Terminal Emulation Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6 Data Management Services

Data Management Services include two distinct areas. The first area is concerned with data and records management technical support provided enterprise-wide and with an enterprise-wide outlook. The second area is concerned with relational database management support for definition, query, and updating of structured data stored in a relational database.

Data Management Services include:

- Metadata Repository
- Metadirectory Services
- Online Analytical Processing (OLAP)
- Data Extraction, Transformation, and Load (ETL) Tools
- Search Services
- Document Management
- Electronic Records Management (ERM)
- Web Content Management (WCM)

- Image and Multimedia Management Systems
- Database Management Systems (DBMS)
- Database Environments
- Data Management Security

#### **4.6.1 Metadata Repository**

An enterprise-wide, central metadata repository provides a mechanism to manage, control, organize, describe, document, standardize, and catalog information about the enterprise information resources. Through the process of capturing metadata about the data stored and extracted, and the sources extracting data; the repository becomes an encyclopedia about the data housed for developers and users. A metadata repository should be sharable across applications. This requires the appropriate tools and published interfaces for importing and exporting metadata from and to other places, such as application development repositories.

A metadata repository supports impact analysis; if the structure of a source file changes, the metadata repository should identify the impact of that schema change for associated applications. A metadata repository provides support for traditional environments, including code parsers, screen and database reverse engineering, copybook and database schema generation, and bridges to / from most traditional development tools, including those which support modeling, code construction, testing, project management and production control.

Repositories are a key technology to manage and reuse metadata across an enterprise with associated definition of issues such as (meta) data ownership rules, and related policies, procedures, standards and methods.

Repositories are the basis for improved information accessibility (e.g. the ease with which users obtain information). Information access and display must be sufficiently adaptable to a wide range of users and access methods, including formats accessible to those with sensory disabilities.

The Judiciary does not currently implement an enterprise data repository. The data architecture is implemented in the software applications which are referenced in Chapter 3 – Application Entities. The documentation may include information and data models which represent internal and external organizational participants, activities, inputs, outputs, flow of information, sequencing, interrelationships between data, and external interfaces. A summary of the Judiciary current data architecture is in Chapter 6 – Current and Target Architecture.

#### *Required Standards:*

- Online Analytical Processing Service Standards
- Database Management System Service Standards
- Data Interchange Service Standards
- Federal Geographic Data standards

**Table 4.6-1: Metadata Repository Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.6-2: Metadata Repository Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**Table 4.6-3: Metadata Repository Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.6-4: Metadata Repository Products to Which the Judiciary Will Evolve**

Vendor	Product	Function	Judiciary Platform	Scope

#### 4.6.2 Metadirectory Services

Metadirectories attempt to solve directory integration problems. The term metadirectory was coined by the Burton Group in 1996 and defined as a “directory [service] that can integrate multiple directory services within an organization.” Thus, a metadirectory is a directory of directories that acts as the authoritative source for information about a network, applications, and users. By synchronizing with the other directories on a network, a metadirectory may allow changes to be made to one database. The metadirectory then propagates this information to other directory services within an organization.

The Burton Group outlined a specific series of processes and characteristics for metadirectory products. However, these were defined before such products existed. When metadirectory products appeared on the market, they were not necessarily designed with all of these characteristics in mind. As a result, many metadirectory product vendors have adopted a broader definition of metadirectory than the Burton Group proposed.

The Gartner Group defines mainstream metadirectory products as providing: multidirectional synchronization between directories, databases, and other types of user information stores. Optionally, they allow a unified view of the information they are synchronizing (a “metaverse”), allowing applications (and potentially, users) to access one directory (the metaverse) for all pertinent information instead of accessing multiple applications.

Some metadirectory products only provide a unified view of information contained in multiple directories or databases and do not provide synchronization as a core capability. Products in this space are often termed “virtual directories”.

Some metadirectory products are actually transaction-oriented infrastructures that enable information system organizations to drive their own synchronization needs. Many products in

this category also support tie-ins to middleware products or scripting interfaces. Most of these products do not maintain a persistent store or persistent joins between the various data sources. They act on a transactional basis, pushing changes directly into other directories.

Metadirectories are not a universal solution for all directory integration problems. They do not always provide password management or synchronization capabilities. They do not enable single sign-on in an enterprise and they provide only limited (if any) capabilities for auditing and reporting. Additional products are normally implemented in addition to a metadirectory product to achieve these goals.

**Table 4.6-5: Metadirectory Service Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.6-6: Metadirectory Service Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

### 4.6.3 Online Analytical Processing (OLAP)

Online analytical processing (OLAP) is a category of software technology that enables analysts, managers and executives to gain insight into data. Through fast, consistent, interactive access to a wide variety of possible views of information, transformed raw data reflects the real dimensionality of the enterprise as understood by the user.

Key OLAP capabilities include:

- Drill/roll up/down – Drilling down or up is a specific analytical technique whereby the user navigates among levels of data ranging from the most summarized (up) to the most detailed (down). The drilling paths may be defined by the hierarchies within dimensions or other relationships that may be dynamic within or between dimensions.
- Slice and Dice – The user-initiated process of navigating by calling for page displays interactively, through the specification of slices via rotations and drill down/up.

OLAP is a technology closely related to warehouse or Database Management System (DBMS). OLAP may be applied to data from any source, but most often from a data warehouse. As a strategic technology, data warehouse is employed to organize and store enterprise data in a fashion that supports OLAP and other analytical technologies. DBMS is a foundation technology for data warehouse. OLAP transforms data warehouse data into strategic information.

The OLAP architecture consists of the following major components: 1) the Database Management System (DBMS), Relational DBMS (RDBMS) and/or specialized Multidimensional DBMS (MDDDBMS); 2) the multidimensional data model, and 3) OLAP end-user desktop services. RDBMS based OLAP systems are ROLAP; MDDDBMS-based systems are Multidimensional OLAP (MOLAP), and combined OLAP systems are referred to as hybrid

OLAPs. A specialized OLAP engine product may or may not be used depending on the end-user requirements for complexity, scalability, and performance.

A multidimensional data model is developed by extracting data from defined data sources, and transforming it to fit into the model. The model organizes business data as a collection of dimensions, such as territory, products, profit, and time. The model is accompanied by another data store referred to as metadata. Metadata is data which describes the data stored in the model, as well as other application data which are not model elements.

GUI-based OLAP front-end desktop applications are referred to as the Enterprise Business Intelligent (EBI) Portal Service layer. They provide end-user access and analytical functions that are supported by the multidimensional data model, which may be hosted on the client, through a direct DBMS Server OLAP interface, or an OLAP Server Engine.

*Required Standards:*

- ISO/IEC 9075-5/Amd1: 2001 Online Analytical Processing (SQL/OLAP)
- ISO/IEC 9075-10:2000 Information technology -- Database languages -- SQL -- Part 10: Object Language Bindings (SQL/OLB)  
<http://webstore.ansi.org/ansidocstore/find.asp>
- JDBC 2.0  
<http://java.sun.com/products/jdbc/>.
- Data Interchange Service standards
- JOLAP, <http://jcp.org/en/jsr/detail?id=069>

**4.6.3.1 (OLAP) Servers**

OLAP services can be accessed directly through a DBMS without a separate OLAP server. However, OLAP servers provide back-end OLAP capabilities such as multi-user read and write access, large-scale data capacity, robust analytical calculations, flexible data navigation, and consistent response times in network centric environments. Relational DBMS vendors provide back-end ROLAP capabilities bundled with the DBMS products, and the OLAP services may be implemented on a DBMS server or a separate OLAP server. The DBMS vendor may additionally provide some level of MOLAP services to support more complex multidimensional analysis and improved performance. Additionally, OLAP Server vendors provide hybrid OLAP engines that are implemented on an OLAP server for several reasons. For instance, data must come from a heterogeneous DBMS environment or the on-demand ad hoc analysis is very complex and can be improved through analysis algorithms. They can also be used when the data and user volumes require the scalability which is inherent in OLAP engines designed with a multi-tier architecture as well as specialized design features such as partitioning for parallel processing and distribution of OLAP application models across LANs and WANs.

**Table 4.6-7: OLAP Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.6-8: OLAP Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

**4.6.3.2 Desktop and Online Analytical Processing (OLAP / DOLAP)**

The OLAP Enterprise Business Intelligence (EBI) Portal service layer provides a single point of personalized access or a ‘portal’ to content to users and a single point of delivery and management of this content. The content may include data stored in the OLAP Model as well as content from any document or report through the original generation software product and format or through an XML format and URL reference. EBI Portal services include query, visualization, report generation, and publication and/or web content distribution. EBI Portal services can be integrated directly with the DBMS or through an OLAP server. EBI Portal services may be provided as part of an application package.

**Table 4.6-9: OLAP/DOLAP Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Crystal Decisions</a>	Crystal Reports 8, 9	Query / Reporting	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	

**Table 4.6-10: OLAP/DOLAP Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**4.6.4 Data Extraction, Transformation, and Load (ETL) Tools**

Extraction, transformation, and migration tools are used to copy data from legacy data sources into long-term relational databases, and short-term reporting tool databases. Transformation tools, which put data in more understandable or consistent formats, reduce the manual effort involved in resolving data replication or errors. Statistical analysis tools support transformation, data integrity assessment, and data extraction.

**Table 4.6-11: ETL Tool Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.6-12: ETL Tool Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
Business Objects	Data Integrator	ETL	X86-based servers, Linux	ALL

#### 4.6.5 Search Services

Full-text searching provides a mechanism for users to look across a collection of documents without having to individually look at all of them. For full-text search to work, the documents must have the text available so that software tools can find it. A document of pictures of text, such as a scanned document, is not searchable.

Optical Character Recognition (OCR) can be run on images of text but there is a sizeable error rate for the process. Even with a 2 percent error rate, which is considered good for OCR, there will be numerous errors per page. This is generally not acceptable within the legal community.

**Table 4.6-13: Full-Text Search Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Thunderstone Software</a>	Webinator	Search Engine	x86-based servers, Solaris 7	ECF <sup>1</sup>

**Table 4.6-14: Full-Text Search Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

#### 4.6.6 Document Management

Document management tools are used to automate business processes and streamline workflows to improve operations, facilitate data exchange, and enhance text and image data dissemination. Document management systems include paper and electronic document tracking, conversion, and configuration management functions as well as electronic document authoring. A document management system's functions may integrate with or overlap with other service entities such as development tools, supporting applications, and database management systems. The Document Management Alliance (DMA) organization is a task force of the Association for Information and Image Management (AIIM) International which is made up of more than 50 commercial and government organizations, including users, vendors, systems integrators, consultants, and industry analysts. DMA is dedicated to defining interoperability standards for document management products.

The Document Management Alliance (DMA) specification defines a vendor-neutral, distributed object framework and interface standard that allows document management systems from different vendors to interoperate, and a front-end application to interact with a document management server. The DMA standardization includes cross-library document search and access, document creation and deletion, check in/out, versioning, multilingual character support, hierarchical folders, and relationships between documents.

An Open Document Management API (ODMA API) is a standardized, platform-independent high-level interface between desktop applications and document management systems (DMSs). It specifies a set of interfaces that applications can use to initiate actions within a DMS.

---

<sup>1</sup> ECF: CM/ECF waiver

*Required Standards:*

- Document Management Alliance Specification (DMA) v1.0  
<http://www.infonuovo.com/DMware/>
- Open Document Management API (ODMA) v2.0
- Extensible Markup Language (XML) Version 1.0 - XML Working Group under the auspices of the World Wide Web Consortium (W3C).  
<http://www.w3c.org/>

**Table 4.6-15: Document Management Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
EMC	Documentum	Document and workflow management	X86Windows -	

**Table 4.6-16: Document Management Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
<a href="#">WorkDynamics Technologies</a>	CcmMercury	Imaging and Workflow		AO
<a href="#">EiStream Technologies</a>	OPEN/Image			AO
<a href="#">IBM</a>	Lotus Domino.Doc	Workflow	x86-based server, Linux	AO
<a href="#">TMSSequoia</a>	Prizm Plug-in	Browser Plug-In to Handle Images	x86-based workstation, MS Windows 2000, XP	AO
<a href="#">TMSSequoia</a>	GrayFix <sup>1</sup>	Improves grayscale images		AO
Pegasus Software	ImageN V 3.0 <sup>1</sup>			AO
<a href="#">EMC</a>	Documentum	Document management and Workflow		AO

#### 4.6.7 Electronic Records Management

An electronic record management system (ERM) supports the objectives of capturing, organizing, appropriately preserving or destroying and classifying record and non-record digital assets. From the perspective of the archivist, ERM extends to documents that are records, electronic or not, as well as other electronic documents that are not records. Thus, ERM encompasses information across a wide range of technologies and media, for example, paper documents which begin life digitally, hand or typewritten forms, official e-mail, websites, voice mail and telephone messages, photographs, architectural drawings, research databases, and financial systems. To effectively manage these documents, files that share common metadata such as subject and organization source should be related logically regardless of their physical media; further, Document management should be integrated in this process in order to provide physical and logical oversight.

*Required Standards:*

- Document Management System service standards
- Database Management System service standards
- Data Interchange service standards
- DoD Records Management Application Standard (DoD 5015.2-STD)  
<http://jitic.fhu.disa.mil/recmgt/standards.htm>

**Table 4.6-17: ERM Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.6-18: ERM Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**Table 4.6-19: ERM Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
<a href="#">Zasio</a>	Versatile Enterprise	Records Management		AO

#### **4.6.8 Web Content Management (WCM)**

Content delivery-centric approaches focus on content entry / page templates. These templates separate format from content stored in a repository and allow central control of site design elements. In particular they facilitate the creation of branding and appearance standards and ensure that content presentation consistently adheres to these standards. The number and type of templates used may be driven by user profiles, group membership, or output channel(s). Content input is generally accepted in text, HTML, XML, and some common office suite formats (e.g. Microsoft Word). Pages are deployed based on business logic and may be viewable across a variety of browsing devices from standard PC-based browsers, to personal digital assistants (PDAs), and, potentially, wireless phones. Content analytic-centric approaches focus on reporting and analysis and generally include tools / utilities to facilitate these needs.

Important additional WCM system features include:

- Compliance with open standards such as Extensible Markup Language (XML) and Java 2 Enterprise Edition (J2EE)
- Browser-based interfaces that facilitate client platform-independent content entry
- Support for versioning, archiving, and site roll-back
- The ability to link to external data sources through Open Database Connectivity (ODBC) or Java Database Connectivity (JDBC) connectors
- Support for Lightweight Document Application Profile (LDAP)
- Conformity to robust, existing or planned, security and backup / recovery architectures

- Support for Section 508 accessibility standards
- Multi-language content compatibility through Unicode support

The move towards Web-centric platforms and technologies has led to the adoption of Internet standards such as HTML and DHTML, XML, and the World Wide Web Distributed Authoring and Versioning) ([WebDAV](#)). Document management software vendors, including WCM vendors, have adopted a number of interface and interoperability standards, including the Document Management Alliance’s DMA 1.0 specification, the Open Document Management API (ODMA) standard sponsored by the Association for Information and Image Management (AIIM). Of these, the preferred integration standards are web-based standards, particularly WebDAV.

Extensible Markup Language (XML) is a simplified subset of SGML that is rapidly becoming the universal format for defining and managing complex data on the web. It is being heralded as the next-generation markup language for the Web. XML provides a standard format for describing different types of data and their relationships. It separates content from style, thus enabling distribution to multiple media or platforms. Intended primarily to meet the needs of Web content providers, XML provides a method of defining markups, vendor-neutral data exchange, and media-independent publishing.

WebDAV is an interface standard that defines the syntax used by an authoring tool when interacting with a Web server. It is a set of extensions to the HTTP which allows users to collaboratively edit and manage files on remote web servers. The WebDAV standard was approved in December 1998. It is replacing ODMA as the predominant integration standard for document management applications. Web authoring tools also contain a subset of web content management capabilities. For web authoring tool information refer to Section 4.4.5.3.

*Required Standards:*

- Web related Software Engineering Service Standards
- Web-related Data Interchange Service Standards
- Web-related Network Communications Protocol Standards
- RFC 2518 WEBDAV (World Wide Web Distributed Authoring and Versioning) HTTP Extensions for Distributed Authoring and Versioning  
<http://www.webdav.org/> or <http://www.ietf.org/ids.by.wg/webdav.html>.

**Table 4.6-20: Web Content Management Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
IBM	Filenet	Content Management	X and windows	

**Table 4.6-21: Web Content Management Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**Table 4.6-22: Web Content Management Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

#### 4.6.9 Image and Multimedia Management Systems

An image management system captures a graphic representation of an object in a digitized image format, manages those images, and integrates them with computer-based distribution. Document imaging is a technology that converts paper images such as photographs into an electronic form where it can be automated using standard computer technology. The imaging technology is used to scan, capture, create, crop, compress, index, store, retrieve, annotate, display, print, and manipulate image data and documents. The digital images can then be electronically filed and be quickly and easily searched and retrieved using the index. After images or other formats of multimedia are created, effective management is key for maximizing digitized media assets. Digital asset management is a category of software addressing media import, catalog, search, download, and intellectual property protection. For a general discussion on Multimedia technologies, refer to:

<http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2013.htm>

*Required Standards:*

- CompuServe’s [Graphics Interchange Format \(GIF\) specification](#).
- Adobe’s [Tagged Image File Format \(TIFF\) specification](#).
- Joint Photographic Experts Group Compression Specification - JPEG (also ANSI/ISO IS10918: 1992)
- World Wide Web’s [Portable Network Graphics \(PNG\) specification](#).
- [Zsoft’s PCX specification](#).
- Adobe’s [Photoshop specification](#).
- Microsoft’s [WAVJoint Photographic Experts Group Compression Specification - Standard: Digital Compression and Coding of Continuous-Tone Still Images specification](#).
- ISO MPEG Standards: [ISO/IEC-11172](#), [ISO/IEC-13818](#), [ISO/IEC-14496](#), [ISO/IEC JTC1/SC29/WG11](#), and [ISO/IEC JTC1/SC29/WG11/N5231](#).

**Table 4.6-23: Multimedia Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**Table 4.6-24: Multimedia Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

#### 4.6.10 Database Management Systems (DBMS)

Database Management Systems provide data management services for definition, query, update, administration, and security of structured data stored in a database. A relational database is used for general-purpose data management, especially where applications require flexibility in data structure and access paths.

The primary methodology for standardized access and manipulation is the relational database model. This model commonly uses Structured Query Language (SQL) as the basis for flexible definition, query, update, and administration of structured data stored in a relational database.

*Required Standards:*

- FIPS 127-2 Database Language SQL June 2, 1993 with Change October 4, 1993
- <http://www.itl.nist.gov/fipspubs/fip127-2.htm>
- ISO/IEC 9075-1:2003 SQL -- Part 1: Framework (SQL/Framework)
- ISO/IEC 9075-2:2003 SQL -- Part 2: Foundation (SQL/Foundation)
- ISO/IEC 9075-3:2003 SQL -- Part 3: Call-Level Interface (SQL/CLI)
- ISO/IEC 9075-4:2003 SQL -- Part 4: Persistent Stored Modules (SQL/PSM)
- ISO/IEC 9075-5:1999 SQL -- Part 5: Host Language Bindings (SQL/Bindings)
- ISO/IEC 9075-5:1999/Amd 1:2001/Cor 1:2003
- ISO/IEC 9075-5:1999/Cor 2:2003
- ISO/IEC 9075-5:1999/Amd 1:2001 Online Analytical Processing (SQL/OLAP)
- ISO/IEC 9075-9:2003 SQL -- Part 9: Management of External Data (SQL/MED)
- ISO/IEC 9075-10:2003 SQL -- Part 10: Object Language Bindings (SQL/OLB)
- ISO/IEC 9075-11:2003 SQL -- Part 11: Information and Definition Schemas (SQL/Schemata)
- ISO/IEC 9075-13:2003 SQL -- Part 13: SQL Routines and Types Using the Java TM Programming Language (SQL/JRT)
- ISO/IEC 9075-14:2003 SQL -- Part 14: XML-Related Specifications (SQL/XML)
- ISO/IEC 9579:2000 SQL -- Remote Database Access for SQL with security Enhancement
- ISO/IEC 13249-1:2002 SQL Multimedia and Application Packages -- Part 1: Framework
- ISO/IEC 13249-2:2003 SQL Multimedia and Application Packages -- Part 2: Full-Text
- ISO/IEC 13249-2:2000/Cor 1:2003
- ISO/IEC 13249-3:2003 SQL Multimedia and Application Packages -- Part 3: Spatial
- ISO/IEC 13249-3:1999/Cor 1:2003
- ISO/IEC 13249-5:2003 SQL Multimedia and Application Packages -- Part 5: Still Image

- ISO/IEC 13249-5:2001/Cor 1:2003
- ISO/IEC 13249-6:2002 SQL Multimedia and Application Packages -- Part 6: Data Mining
- ANSI NCITS 331.1-1999 SQLJ - Part 1: SQL Routines using the Java (TM) Programming Language
- ANSI NCITS 331.2-2000 SQLJ Part 2: SQL Types using the Java TM Programming
- JDBC <http://java.sun.com/products/jdbc/>
- ODBC <http://msdn.microsoft.com/library/en-us/odbc/htm/dasdkodbcoverview.asp>

**Table 4.6-25: DBMS Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">IBM</a>	Informix 7, 9	Multi-user Relational database	x86-based servers, Solaris 7	
<a href="#">Microsoft</a>	Access 95, 97, 2000, XP	For less than 10 concurrent users on a server database use only, including minimal development work	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	FoxPro		x86-based server, MS Windows NT, 2000	AO
<a href="#">Microsoft</a>	SQL Server 6.0, 6.5, 7.0, 2000	Multi-user Relational database	x86-based server, MS Windows NT, 2000	AO
<a href="#">Computer Associates</a>	IDMS	Hierarchical Database	Mainframe	AO

**Table 4.6-26: DBMS Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
<a href="#">IBM</a>	Informix 9	Multi-user Relational Database	x86-based server, Linux	
<a href="#">Microsoft</a>	Access XP	Database for Desktop use	x86-based workstation, MS Windows 2000, XP	

**Table 4.6-27: DBMS Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
MySQL	MySQL	Multi-user Relational Database	x86-based server, Linux	

#### 4.6.11 Database Environments

A database environment provides an interface to access data stored in diverse databases and non-Structured Query Language (SQL) data repositories. A database environment also supports distributed computing services and systems management functions such as transaction process monitoring (refer to Distributed Computing Services), object request broker, load balancing, and distributed backup recovery services.

Remote Database Access (RDA) is used to establish a remote connection between an RDA client and an RDA server to promote the interconnection of applications and the interoperability of database management systems in a heterogeneous environment. RDA services consist of dialogue management, association control, resource handling, and data language services between client and server. Association control includes making a connection to a specific database at the server site. SQL statements are sent in character strings with a separate list of input parameters, and the resulting data or exception conditions are returned.

Java Database Connectivity (JDBC) is a DBMS independent API that enables / supports applications that need access to the database. The JDBC specification is based on the X/Open SQL Call Level Interface (CLI) that defines how client-server interactions are implemented for database systems.

Open Database Connectivity (ODBC) is an API for database access on Linux, Unix, and Microsoft platforms. It is also based on the Call Level Interface (CLI) specifications from X/Open and ISO/IEC for database APIs and uses SQL as its database access language.

The Open Database Connectivity (ODBC) and Java Data Base Connectivity (JDBC) drivers provide a uniform interface tool for accessing data stored in the data repositories.

##### *Required Standards:*

- FIPS 127-2 Database Language SQL June 2, 1993 with Change October 4, 1993  
<http://www.itl.nist.gov/fipspubs/fip127-2.htm>
- ISO/IEC 9075-1:2003 SQL -- Part 1: Framework (SQL/Framework)
- ISO/IEC 9075-2:2003 SQL -- Part 2: Foundation (SQL/Foundation)
- ISO/IEC 9075-3:2003 SQL -- Part 3: Call-Level Interface (SQL/CLI)
- ISO/IEC 9075-4:2003 SQL -- Part 4: Persistent Stored Modules (SQL/PSM)
- ISO/IEC 9075-5:1999 SQL -- Part 5: Host Language Bindings (SQL/Bindings)
- ISO/IEC 9075-5:1999/Amd 1:2001/Cor 1:2003
- ISO/IEC 9075-5:1999/Cor 2:2003
- ISO/IEC 9075-5:1999/Amd 1:2001 Online Analytical Processing (SQL/OLAP)
- ISO/IEC 9075-9:2003 SQL -- Part 9: Management of External Data (SQL/MED)
- ISO/IEC 9075-10:2003 SQL -- Part 10: Object Language Bindings (SQL/OLB)
- ISO/IEC 9075-11:2003 SQL -- Part 11: Information and Definition Schemas (SQL/Schemata)
- ISO/IEC 9075-13:2003 SQL -- Part 13: SQL Routines and Types Using the Java TM Programming Language (SQL/JRT)

- ISO/IEC 9075-14:2003 SQL -- Part 14: XML-Related Specifications (SQL/XML)
- ISO/IEC 9579:2000 SQL -- Remote database access for SQL with Security Enhancement
- ISO/IEC 13249-1:2002 SQL Multimedia and Application Packages -- Part 1: Framework
- ISO/IEC 13249-2:2003 SQL Multimedia and Application Packages -- Part 2: Full-Text
- ISO/IEC 13249-2:2000/Cor 1:2003
- ISO/IEC 13249-3:2003 SQL Multimedia and Application Packages -- Part 3: Spatial
- ISO/IEC 13249-3:1999/Cor 1:2003
- ISO/IEC 13249-5:2003 SQL Multimedia and Application Packages -- Part 5: Still Image
- ISO/IEC 13249-5:2001/Cor 1:2003
- ISO/IEC 13249-6:2002 SQL Multimedia and Application Packages -- Part 6: Data Mining
  
- ANSI NCITS 331.1-1999 SQLJ - Part 1: SQL Routines Using the Java (TM) Programming Language
- ANSI NCITS 331.2-2000 SQLJ Part 2: SQL Types using the Java TM Programming
  
- JDBC  
<http://java.sun.com/products/jdbc/>
  
- ODBC  
<http://msdn.microsoft.com/library/en-us/odbc/html/dasdkodbcoverview.asp>

**Table 4.6-28: Database Environment Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
IBM	Informix 7, 9		x86-based servers, Solaris 7	
<a href="#">Unify</a>	Unify		x86-based servers, Solaris 2.5.1	

**Table 4.6-29: Database Environment Preferred Product for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">IBM</a>	Informix 9 <sup>1</sup>		x86-based servers, Linux	

#### 4.6.12 Data Management Security

Data Management Security mechanisms provide three separate functions: confidentiality, integrity, and authorization. Integrity insures that only appropriate values are inserted into the

<sup>1</sup> Informix will continue to be the Judiciary database for the life of the present contract. A waiver may be considered if third-party products that are required by a project will not support Informix. The third-party products must either be on the TRM Preferred/To Be list or will have to get waivers themselves.

database. Authorization limits access, modification, and deletion to those with appropriate rights.

**Confidentiality**—SQL defines standard components and facilities for relational database management systems. The components of a SQL database are a schema, tables, and views. A schema describes the structure of related tables and views. Tables store the data in the database; they consist of rows and columns. Each row contains a set of data elements organized by and associated with a set of columns; each column contains many instances of a single data element. Views are derived tables and may be composed of a subset of a table or the result of table operations, such as a join of different tables.

**Integrity**—Data integrity is addressed by a variety of data constraints specified in the database schema. These constraints describe relationships between tables, relationships between rows in a table, and permissible values for elements. Relationships between tables, or between rows in a table are known as table constraints. Range checks and other specifications for data values are element constraints.

**Authorization** – Within a database different users will have different rights to create, use, modify, and remove the data. These rights are defined by the application requirements and can be implemented within most databases. One simple mechanism is to set privileges by table by setting select, delete, update, and insert by user. More subtle approaches are to use views or stored procedures. These allow for more discrimination based on the values of the data.

The operating system is responsible for guaranteeing the simple integrity of the data and preventing denial of service. Deadlock (and denial of service) is one possible result of such concurrent transactions; loss of data integrity is another. Such actions can result in loss of integrity (e.g., improper modification of data) or confidentiality (e.g., by circumventing internal access controls of SQL). For more information see NIST Special Publication 800-8.

*Required Standards:*

- ISO/IEC 9579:2000 Information technology – Remote database access for SQL with security enhancement  
<http://webstore.ansi.org/ansidocstore/find.asp?>

**Table 4.6-30: Data Management Security Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.6-31: Data Management Security Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

## 4.7 Data Interchange Services

Data interchange services provide specialized support for the interchange of information including format and semantics of data entities between applications on the same or different platforms. Data interchange services describe the following data exchange standards and formats:

- Financial and Human Resources Technical Standards
- Library Interchange Standards
- Unicode Standard
- Markup Languages
- Portable Document Format (PDF)
- File Compression Formats
- Office Automation File Formats
- Calendar Date and Ordinal Date Interchange Format
- Vector Graphics
- Raster Image Interchange Format
- Tag Image File Format (TIFF)
- Joint Photographic Experts Group (JPEG)
- Motion Picture Experts Group (MPEG)
- Electronic Data Interchange (EDI)
- Computer-Aided Design (CAD) Data

### 4.7.1 Financial and Human Resources Technical Standards

The Joint Financial Management Improvement Program (JFMIP) is a cooperative undertaking of the U.S. Department of the Treasury, the General Accounting Office, the Office of Management and Budget, and the Office of Personnel Management working in cooperation with other agencies. The program guides and promotes strategies and standards for financial management improvements across the government as well as revising the federal government's requirements, definition, testing, and acquisition process. Their primary target is core financial systems and their objectives are to develop systems requirements, communicate and explain federal and agency needs, provide agencies and vendors information to improve financial systems, ensure that products meet relevant system requirements, and simplify the procurement process.

The Federal Accounting Standards Advisory Board (FASAB) is sponsored by three of the principles of the JFMIP – The Secretary of the Treasury of the United States, The Comptroller General of the United States, and the Director of the Office of Management and Budget. FASAB promulgates accounting principles for federal government reporting entities, issuing publications including exposure drafts, the volume of original pronouncements (“Codification”), as well as newsletters, minutes, and meeting agendas.

#### *Required Standards:*

- The Joint Financial Management Improvement Program (JFMIP) <http://www.jfmip.gov/jfmip/>
- The Federal Accounting Standards Advisory Board (FASAB) <http://www.fasab.gov/>

**Table 4.7-1: JFMIP Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">AMS</a>	Momentum	Accounting	x86-based, Solaris 7	FAS <sup>1</sup> CJA <sup>2</sup>
<a href="#">AMS</a> (change AMS to CGI)	FFS	Accounting	Mainframe	AO <sup>3</sup>

**Table 4.7-2: JFMIP Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
PeopleSoft		Human Resources	HP-UX	HRMIS
<a href="#">AMS</a>	Momentum	Accounting	x86-based, Linux	FAS <sup>1</sup> CJA <sup>2</sup>

**Table 4.7-3: JFMIP Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
PeopleSoft		Human Resources	Linux	HRMIS

#### 4.7.2 Library Interchange Standards

Machine-Readable Cataloging (MARC) 21 is the latest implementation of the MARC/USMARC data standards managed by the U.S. Library of Congress. Records refer to records where one particular type of machine, a computer, can read and interpret the data in the cataloging record. A "cataloging record" is defined as a bibliographic record, or the information traditionally shown on a catalog card. The record includes a description of the item, main entry and added entries, subject headings, and the classification or call number. (MARC records often contain a lot of additional information.)

The U.S. MARC Advisory Committee advises the Library of Congress concerning changes to the MARC 21 formats. The Library of Congress maintains the MARC 21 formats for Bibliographic, Authority, Holdings, Classification, and Community Information data for the MARC 21 user community.

The U.S. MARC Advisory Committee includes the American Library Association's (ALA) Machine-Readable Bibliographic Information (MARBI) committee, U.S. national libraries, the National Library of Canada and the National Library of Australia; as well as the large bibliographic networks such as the Online Computer Library Center (OCLC) and Research Libraries Information Network (RLIN), library associations such as the Music Library Association, Special Libraries Association, and library system vendors.

*Required Standards:*

<sup>1</sup> FAS: FAS4T COTS product

<sup>2</sup> CJA: CJA COTS product

<sup>3</sup> AO: Mainframe COTS product

- MARC (Machine-Readable Cataloging) <http://www.loc.gov/marc/>  
<http://lcweb.loc.gov/marc/status.html>
- ANSI Z39.2, Information Interchange Format BIBLIOGRAPHIC INFORMATION INTERCHANGE
- ANSI X3.4, Code for Information Interchange (ASCII) CODED CHARACTER SETS-7-BIT AMERICAN NATIONAL STANDARD
- ANSI Z39.47, Extended Latin Alphabet Coded Character Set for Bibliographic Use (ANSEL)
- [ISO 2709, Format for Information Exchange](#)
- [NISO Z39.71, Holdings Statements for Bibliographic Items](#)
- [Z39.50](#) Information Retrieval Standard (copy to search -- proposals for searching between information systems; used with SIRIS)
- UNICODE is based on ISO 10646, Universal Character Set (UCS)
- ALA (American Library Association) Character set
- ANSI Z39.56, Serial Item and Contribution Identifier (SICI)
  - CODABAR Barcode standards
  - Z39.19, Guidelines for Construction, Format, and Management of Monolingual Thesauri (pertains to AFA thesaurus)
- Dublin Core: This is ANSI Z39.85, Dublin Core Metadata Element Set Dublin Core Metadata Element Set, Version 1.1: Reference Description, 1999-07-02, <http://dublincore.org/documents/dces/>
- NISO 2001-07-02, (the NISO version of the Dublin Core element set)
- ISO/IEC 11179 [ISO11179] standard for the description

**Table 4.7-4: Library Interchange Standards Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.7-5: Library Interchange Standards Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

### 4.7.3 Unicode Standard

The Unicode Standard is the universal character-encoding scheme for written characters and text. The Unicode Worldwide Character Standard is a character coding system designed to support the interchange, processing, and display of the written text of the diverse languages of the modern world. In addition, it supports classical and historical texts of many written languages. With Unicode, the information technology industry gains data stability by not proliferating character sets, greater global interoperability and data interchange, and simplified software and reduced development costs. The encoding system allows computer systems to exchange text information unambiguously because each character is encoded as a single code point.

While modeled on the ASCII character set, the Unicode Standard goes far beyond ASCII's limited ability to encode only the upper- and lowercase letters A through Z and a handful of additional characters. It provides the capacity to encode all characters used for the written languages of the world – more than 1 million. No escape sequence or control code is required to specify any character in any language. Unicode character encoding treats alphabetic characters, ideographic characters, and symbols equivalently, which means they can be used in any combination and with equal facility.

*Required Standards:*

- Unicode Standards
- ISO/IEC 6937 and ISO/IEC 8859 families of standards
- SGML standard ISO/IEC 8879
- Bibliographic standards ISO 5426
- ANSI Z39.64, KS C 5601, JIS X 0209, JIS X 0212, GB 2312, and CNS 11643
- Industry code pages and character sets from Adobe, Apple, Fujitsu, Hewlett-Packard, IBM, Lotus, Microsoft, NEC, and Xerox
- References section of The Unicode Standard, Version 3.0, <http://www.unicode.org/unicode/standard/standard.html>
- Unicode Character Set (UCS) - ISO/IEC 10646-1:2000 Information Technology-- Universal Multiple-Octet Coded Character Set (UCS)--Part 1: Architecture and Basic Multilingual Plane, which is also known as the Universal Character Set (UCS)

**Table 4.7-6: Unicode Standard Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.7-7: Unicode Standard Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

## 4.7.4 Markup Languages

### 4.7.4.1 Standard Generalized Markup Language

Standard Generalized Markup Language (SGML) is a device-independent standardized electronic interchange format for managing mixed-mode document structure and content. It is used to define, describe, individually store the structure and contents of, and exchange specific documents. SGML formally defines the grammar of languages for document markup. SGML provides a way to specify what is required or optional, and how the markup is distinguished from the text. This is accomplished by means of two SGML components: SGML tags, and Document Type Definitions (DTD). SGML tags function as labels, identifying parts of documents, such as chapters, paragraphs, and section headings. By tagging the parts of the document using SGML standards, users may tailor retrieval and viewing of the document to specific needs. The DTD defines a document structure by defining relationships between tags.

SGML differs from document conversion programs that preserve only document formats. SGML preserves document content, or information, as well as document structure, or the relationship among the document data, and facilitates document publishing.

[SGML](#) is defined by ISO 8879. In 1986, SGML became an international standard for defining descriptions of the structure and content of different types of electronic documents. SGML has been the standard, vendor-independent way to maintain repositories of structured documentation for two decades, but it is not well suited to serving documents over the Web (for a number of technical reasons beyond the scope of this document). These barriers include the lack of widely supported style sheets, complex and unstable software because of SGML's broad and powerful options, and obstacles to interchange of SGML data because of varying levels of SGML compliance among SGML software packages.

*Required Standards:*

- ANSI/ISO 8879:1986, Standard Generalized Markup Language (SGML)  
<http://www.w3c.org/MarkUp/SGML/>

#### **4.7.4.2 Extensible Markup Language )**

Extensible Markup Language (XML) is a markup language for documents containing structured information. A markup language is a mechanism to identify structures in a document. The XML specification defines a standard way to add markup to documents. Structured information contains both content (words, pictures, etc.) and some indication of what role that content plays.

[XML](#) Extensible Markup Language is defined as an application profile of SGML meaning that any fully conformant SGML system will be able to read XML documents. However, using and understanding XML documents *does not* require a system that is capable of understanding the full generality of SGML. XML is, roughly speaking, a restricted form of SGML.

XML specifies neither semantics nor a tag set; it is a meta-language for describing markup languages. XML provides a facility to define tags and the structural relationships between them. Since there's no predefined tag set, there can't be any preconceived semantics. All of the semantics of an XML document will either be defined by the applications that process them or by style sheets.

XML was created so that richly structured documents could be used over the Web. The only viable alternatives, HTML and SGML, are not practical for this purpose. HTML comes bound with a set of semantics and does not provide arbitrary structure. SGML provides arbitrary structure, but is too difficult to implement just for a web browser. Full SGML systems solve large, complex problems that justify their expense. Viewing structured documents sent over the Web rarely carries such justification.

#### **4.7.4.3 Hypertext Markup Language**

Hypertext Markup Language ([HTML](#)) is a subset of SGML. It defines a single, fixed type of document with markup that lets you describe a common class of simple office style reports, with headings, paragraphs, lists, illustrations, etc., and some provision for hypertext and multimedia.

HTML was defined to allow the transfer, display and linking of documents over the Internet and is the key enabling technology for the World Wide Web (WWW). The World Wide Web Consortium (W3C), in conjunction with browser vendors and the WWW community, is constantly working to extend the definition of HTML to allow new tags to keep pace with changing technology and to bring variations in presentation (e.g., style sheets) to the Web. However, these changes are always rigidly confined by what the browser vendors have implemented and by the fact that backward compatibility is paramount. For people who want to disseminate information widely, features supported by only the latest releases of Internet Explorer or Netscape are not useful.

#### 4.7.4.4 Extensible Hypertext Markup Language

Extensible Hypertext Markup Language ([XHTML](#)) is a W3C recommendation for the formulation of HTML 4.0 [HTML] as an application of XML 1.0 [XML]. It is the basis for a family of future document types that extend and subset HTML. A [tutorial on XHTML Modules and Markup Languages](#) was published on 01 August 2001. This tutorial explains how to create XHTML Family modules and markup languages, based on [Modularization of XHTML](#). For further information on XHTML, refer to <http://www.w3c.org/MarkUp/Guide/xhtml-m12n-tutorial/>.

#### 4.7.4.5 Cascading Style Sheets

Cascading Style Sheets (CSS2) is a style sheet language that allows authors and users to attach style (e.g., fonts, spacing, and aural cues) to structured documents (e.g., HTML documents). By separating the presentation style of documents from the content of documents, CSS2 simplifies Web authoring and site maintenance. Refer to <http://www.w3c.org/Style/CSS/> for more information.

#### 4.7.4.6 Extensible Stylesheet Language

Extensible Stylesheet Language (XSL) is a language for expressing style sheets. It consists of three parts: [XSL Transformations](#) (XSLT), a language for transforming XML documents; the [XML Path Language](#) (XPath), an expression language used by XSLT to access or refer to parts of an XML document (XPath is also used by the [XML Linking](#) specification); and XSL Formatting Objects, which is an XML vocabulary for specifying formatting semantics.

An XSL style sheet, as with [CSS](#), is a file that describes how to display an XML document of a given type. XSL and CSS share the functionality and are compatible, although they use a different syntax. XSL style sheet specifies the presentation of a class of XML documents by describing how an instance of the class is transformed into an XML document that uses the formatting vocabulary. For a more detailed explanation of how XSL works, see the [What Is XSL](#) page at <http://www.w3c.org/Style/XSL/WhatIsXSL.html>.

1986	SGML ISO 8879-1986
Nov 1995	HTML 2.0
Nov 1996	Simplified and stripped down SGML draft (dubbed XML)

Jan 1997	HTML 3.2
Aug 1997	XML working draft
Dec 1997	<a href="#">XML 1.0</a> proposed recommendation (revision October 2000) <a href="#">HTML 4.0</a> W3C Recommendation (revision <a href="#">HTML 4.01</a> in Dec 1999. Refer to <a href="http://www.w3c.org/TR/html4/">http://www.w3c.org/TR/html4/</a> )
Feb 1998	<a href="#">XML</a>
Feb 1999	<a href="#">XHTML</a>
May 31, 2001	<a href="#">XHTML 1.1 - Module-based XHTML</a> as a <a href="#">W3C Recommendation</a>

*Required Standards:*

- Document Object Model (DOM) Level 2 HTML Specification Version 1.0, W3C Recommendation 09 January 2003 <http://www.w3c.org/TR/DOM-Level-2/>
- W3C HTML home page, <http://www.w3c.org/MarkUp/>
- HTML 4.01 Specification, W3C Recommendation 24 December 1999, <http://www.w3c.org/TR/html4/>
- XHTML 1.0, XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition), A Reformulation of HTML 4 in XML 1.0, W3C Recommendation 26 January 2000, revised 1 August 2002 <http://www.w3c.org/TR/xhtml1/>
- XHTML 1.1, Module-based XHTML, W3C Recommendation 31 May 2001, <http://www.w3c.org/TR/xhtml11/>
- XML (Extensible Markup Language) 1.0, <http://www.w3c.org/XML/>
- Cascading Style Sheets, level 2, CSS2 Specification, W3C Recommendation 12-May-1998, <http://www.w3c.org/TR/REC-CSS2/>
- The Extensible Stylesheet Language ([XSL](#)), <http://www.w3c.org/Style/XSL/>
- Mathematical Markup Language (MathML) Version 2.0, W3C Recommendation 21 February 2001
- XML schema, W3C recommendation, May 2001, [XML Schema Part 0: Primer](#) , <http://www.w3c.org/TR/xmlschema-0/>  
[XML Schema Part 1: Structures](#) <http://www.w3c.org/TR/xmlschema-1/>  
[XML Schema Part 2: Datatypes](#) <http://www.w3c.org/TR/xmlschema-2/>

For further information, refer to <http://www.w3c.org/XML/>.

**Table 4.7-8: XSL Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.7-9: XSL Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

**4.7.5 Portable Document Format**

Portable Document Format (PDF) is the open de facto standard for electronic document distribution worldwide. The PDF specification was developed and is maintained by Adobe Systems Inc. It offers a method for display and faithful representation of documentation, and is used as a format for electronic document distribution. PDF provides for the final form of information delivered electronically in a standardized platform-independent format. The portable final form of the document is created from the reversible form of the document using conversion algorithms.

PDF is a universal file format that preserves all of the fonts, formatting, colors, and graphics of any source document, regardless of the application and platform used to create it. PDF files can be compact and can be shared, viewed, navigated, and printed exactly as intended by anyone with an Adobe Acrobat Reader. Any document can be converted to PDF, even scanned paper, using Adobe Acrobat software or other PDF generators.

*Required Standards:*

- *Portable Document Format Reference Manual, fourth edition, version 1.4, 2003* by Adobe Systems Incorporated - Industry Standard  
[http://partners.adobe.com/asn/acrobat/docs/File\\_Format\\_Specifications/PDFReference.pdf](http://partners.adobe.com/asn/acrobat/docs/File_Format_Specifications/PDFReference.pdf)
- *Add PDF/A standard*

**Table 4.7-10: PDF Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Adobe Systems</a>	Acrobat Exchange and Distiller 3.01	Administration of PostScript-to-PDF file conversion	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Adobe Systems</a>	Acrobat 4.0, 5.x (Includes Acrobat Distiller and Catalog), 6.0	Convert documents into PDF format, create interactive .pdf documents, create index, searchable, .pdf document collections.	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Adobe Systems</a>	Acrobat Reader 4.0, 5.0, 6.0	Freeware PDF viewer	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Corel</a>	Corel WordPerfect 8, 9, 10, 11	PDF Generator	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	

**Table 4.7-11: PDF Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Adobe Systems</a>	Acrobat 8	Convert documents into PDF format, create interactive .pdf documents, create index, searchable, .pdf document collections	x86-based workstation, MS Windows 2000, XP (check for Linux)	
<a href="#">Adobe Systems</a>	Acrobat Reader 8	Freeware PDF viewer	x86-based workstation, Linux, MS Windows 2000, XP	

#### 4.7.6 File Compression Formats

Software file compression uses algorithms to combine and compress one or multiple files or directories into a single file of a recognized format that may be re-expanded using the same software or other products supporting that format. Compression formats include: *.zip*, *.cab*, *.tar*, *gzip*, *.arj*, *.lzh*, and *.arc*. Many compression suites contain additional features such as browser integration and the ability to create self-extracting (.exe) files that will automatically install software upon execution. For example, zip files are "archives" used for distributing and storing files. Zip files contain one or more files. Usually the files "archived" in a zip are compressed to save space. Zip files make it easy to group files and make transporting and copying these files faster. *.cab*, *.tar*, *.arj*, *.lzh*, and *gzip* files provide most of the benefits of zip files, but use different file formats.

External programs are required for the less frequently used ARJ, ARC, and LZH formats. TAR, Z, GZ, TAZ, and TGZ files are often found on Unix-based Internet sites. TAR stands for "Tape ARchive". This is a file format and does not provide compression; it is used only to group files. Z files are compressed with the compression program. GZ files are gzip files. Z and GZ files cannot contain multiple files. TAZ and TGZ files are TAR files compressed in Z or GZ format. A *.tar.gz* file is simply a bundle of files packaged with TAR, and subsequently compressed with Gzip. Sometimes the extension ".tgz" is used as an abbreviation for ".tar.gz".

For further information on Zip format, please refer to <http://www.eurekais.com/brock/aazip.htm#intro> and <http://www.winzip.com/aboutzip.htm>. For further information on TAR and GZ format, please refer to <http://www.gnu.org/software/tar/tar.html> and <http://www.gzip.org/>.

Some network operating systems also include a file compression option. This feature is intended to maximize available hard drive space by storing all data files in a compressed format, invisibly de-compressing them, when the file is accessed, and compressing when the file is closed. This feature is usually enabled at the volume level.

**Table 4.7-12: Compression Formats for the Judiciary**

Format	Vendor
ZIP format	All platforms
TAR.GZ format	All UNIX operating systems and Linux

**Table 4.7-13: File Compression Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Microsoft</a>	Windows XP	OS enabled compression on files	x86-based workstation, MS Windows XP	
<a href="#">PKWare Inc.</a>	PKZip	File compression	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">WinZip Computing Inc.</a>	Winzip 7.x, 8.x	File compression can handle Zip, TAR, gzip, and CAB files	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
	Compress	File compression	x86-based server, Solaris	
	Gzip	File compression	x86-based server, Solaris	

**Table 4.7-14: File Compression Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.7 Office Automation File Formats

The section identifies structures for files used in word processing, spreadsheet, graphic representation, and e-mail communications that are shared across Judiciary business units.

Rich Text Format (RTF) is a file format that is used for exchange text files between different word processors in different operating systems. The RTF specification uses the ANSI, PC-8, Macintosh, and IBM PC character sets. It defines control words and symbols that serve as a “common denominator” for formatting commands. When a file is saved in the Rich Text Format, the file is processed by an RTF writer which converts the word processor’s markup to the RTF language. When being read, the control words and symbols are processed by an RTF reader. The RTF reader converts the RTF language into the word processor format to display the document.

*Required Standards:*

- RTF standard – Rich Text Format specification version 1.7
- Open Office specification version 2.0

**Table 4.7-15: Office Automation File Format Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Corel</a>	Corel WordPerfect 8, 9 10, 11, 12 <sup>1</sup>	Word processing	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Microsoft Word 95, 97, 2000 XP	Word processing	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Microsoft Excel 95, 97, 2000, XP	Spread sheet	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Microsoft PowerPoint 95, 97, 2000, XP	Presentation	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Microsoft</a>	Microsoft Access 95, 97, 2000, XP	Desktop database	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Zandar</a>	TagWrite	Converts between word processing Formats	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO

**Table 4.7-16: Office Automation File Format Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Corel</a>	Corel WordPerfect 8, 9, 10, 11, 12	Word processing	x86-based workstation, MS Windows 2000, XP	
<a href="#">Microsoft</a>	Microsoft Word XP	Word processing	x86-based workstation, MS Windows 2000, XP	
<a href="#">Microsoft</a>	Microsoft Excel XP	Spreadsheet	x86-based workstation, MS Windows 2000, XP	
<a href="#">Microsoft</a>	Microsoft PowerPoint XP	Presentation	x86-based workstation, MS Windows 2000, XP	
<a href="#">Microsoft</a>	Microsoft Access XP	Desktop database	x86-based workstation, MS Windows 2000, XP	

**Table 4.7-17: Office Automation File Format Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Open source	OpenOffice – check spelling	General Office Automation Products and Conversion	x86-based workstation, Linux, MS Windows 2000, XP	

<sup>1</sup> There are likely to be documents in WordPerfect 4 and 5 formats.

#### 4.7.8 Calendar Date and Ordinal Date Interchange Format

Date interchange format provides a means of representing calendar dates to facilitate interchange of data among information systems.

*Required Standards:*

- American National Standard ANSI X3.30-1997: Representation of Date for Information Interchange (revision of ANSI X3.30-1985 (R1991)).  
[http://web.ansi.org/public/std\\_info.html](http://web.ansi.org/public/std_info.html)
- FIPS PUB 4-2, “Representation of Calendar Date for Information Interchange”, November 15, 1998.
- ISO 8601:2000, *Data Elements and Interchange Formats - Information Interchange – Representation of Dates and Times*  
<http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26780&ICS1=1&ICS2=140&ICS3=30>  
<http://www.itl.nist.gov/fibspubs/fips4-2.html>

**Table 4.7-18: Date Interchange Format Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.7-19: Date Interchange Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.9 Vector Graphics

Scalable Vector Graphics (SVG) is a language for describing two-dimensional graphics in XML. As the name implies, it is a vector representation. Computer Graphics Metafile (CGM) is a graphical data interchange standard that facilitates the transfer of picture description information between different software systems, different graphical devices, and different computer graphics installations. CGM specifies a file format suitable for the description, storage, and communication of picture description information in a device-independent manner. It is a vector format that can include raster bitmap encoding. The adopted CGM standard supports an open systems approach to the interchange format for the storage, interchange, or output of a wide range of graphical pictures (from slides for presentation graphics or business charts to applications-generated diagrams).

*Required Standards:*

- Scalable Vector Graphics (SVG) 1.1 Specification; W3C Recommendation 14 January 2003. <http://www.w3.org/TR/SVG11/>
- ANSI/8632.1-4:1192[1994], ANSI/ISO 8632/Amd.1: 1994, ANSI/ISO 8632:1992/Adm.2: 1995, MIL-D-28003A. FIPS 128-2

**Table 4.7-20: SVG Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Adobe</a>	Photoshop 6.0	Graphics Application	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO <sup>1</sup>
<a href="#">Macromedia</a>	Freehand 10.0	Graphics Application	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO <sup>1</sup>
<a href="#">Macromedia</a>	Fireworks 4.0	Graphics Application	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO <sup>1</sup>

**Table 4.7-21: SVG Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

#### 4.7.10 Raster Image Interchange Format

The Raster Image is a widely implemented facsimile standard for black and white images (i.e., images not containing gray scale or color) and a preferred method for describing, storing, and exchanging gray scale raster-scanned images and illustrations. Raster images may be compressed by using a Run-Length Encoding (RLE) algorithm.

*Required Standards:*

- ISO/IEC 12064-1:1995 International Standardized Profile; and Consultative Committee for International Telephony and Telegraphy (CCITT) Group 4 Raster Image Standard

**Table 4.7-22: Raster Image Interchange Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Informatik</a>	DOC2PIX	Raster Printer Driver	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO <sup>1</sup>

**Table 4.7-23: Raster Image Interchange Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

#### 4.7.11 Tagged Image File Format

Tagged Image File Format (TIFF) is a common format for exchanging raster graphics (bitmap) images between application programs, including those used for scanner images. A TIFF file can be identified as a file with a .tiff or .tif file name suffix. The TIFF format was developed in 1986 by an industry committee, chaired by the Aldus Corporation (now part of Adobe Software). Microsoft and Hewlett-Packard were among the contributors to the format. One of the most

<sup>1</sup> Used by the AO, not entire judiciary

common graphic image formats, TIFF files are commonly used in desktop publishing, faxing, 3D applications, and medical imaging applications. TIFF files can be in any of several classes, including gray scale, color palette, or Red Blue Green (RGB) full color, and can include files with JPEG, LZW (short for Lempel-Zif-Welch), or CCITT Group 4 standard run-length image compression.

Run Length Encoding (RLE) is simple lossless technique originally designed for data compression and later modified for facsimile. RLE compresses an image based on "runs" of pixels. Although it works well on black-and-white facsimiles, RLE is not very efficient for color video, which has few long runs of identically colored pixels.

*Required Standards:*

- TIFF (Tag Image File Format) Revision 6.0  
<http://partners.adobe.com/asn/developer/PDFS/TN/TIFF6.pdf>

**Table 4.7-24: TIFF Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Lincoln</a>	EPFaxPS 2.0	Converts PostScript, PDF to TIFF	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO

**Table 4.7-25: TIFF Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Deployment Platform	Scope
TBD				

**4.7.12 Joint Photographic Experts Group**

The Joint Photographic Experts Group (JPEG) is a standard that has been adopted by two international standards organizations: the International Telecommunication Union (ITU) (formerly CCITT) and the International Organization for Standardization, the ISO. JPEG is most often used to compress still images through Discrete Cosine Transformation (DCT) analysis. DCT first divides the image into blocks and then converts the colors and pixels into frequency space by describing each block in terms of the number of color shifts (frequency) and the extent of the change (amplitude). Because most natural images are relatively smooth, the changes that occur most often have low amplitude values. In other words, images have many subtle shifts among similar colors but few dramatic shifts between very different colors. Three elements are specified in the JPEG standard: an encoder, a decoder, and an interchange format. JPEG is a standardized method for compression and coding of continuous-tone (gray scale or full color) digital still image data and is appropriate for a wide range of applications. Designed to compress "real-world" scenes, the primary use is as a standardized way of compressing and storing both 24-bit color and gray-scale images. With this specification, compressed formatted image files are more efficiently transmitted across networks. JPEG is not applicable to bi-level image data. Because it is considered to be a poor compression technology, in which image information is lost in the compression process, JPEG is not used on images requiring precise reconstruction, such as satellite images or maps. JPEG has been adopted for motion video.

*Required Standards:*

- Joint Photographic Experts Group Compression Specification - JPEG (also ANSI/ISO IS10918-1 (ITU-T T.81)) Standard: Digital Compression and Coding of Continuous-Tone Still Images  
<http://www.jpeg.org/>

**Table 4.7-26: JPEG Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">AccuSoft</a>	ImageGear	Image Display and Conversion	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO

**Table 4.7-27: JPEG Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

#### 4.7.13 Motion Picture Experts Group

Moving Picture Experts Group, or MPEG, is the name given to a family of [International Standards](#) used for coding audio-visual information in a digital compressed format. The MPEG family of standards includes MPEG-1, MPEG-2 and MPEG-4, formally known as [ISO/IEC-11172](#), [ISO/IEC-13818](#) and [ISO/IEC-14496](#). The MPEG could be considered as a compression mechanism to handle multimedia applications on video, graphics, and moving image. It is used as a standard for both storage and transmission of moving imagery data. The MPEG compression standard is intended for full-motion image compression for high-performance entertainment-quality video. MPEG is used in conjunction with mass media such as hard drives, CD-ROM, and other optical storage devices: writable CD, Digital Audio Tape (DAT), and network servers. MPEG compression techniques are geared to such applications as electronic publishing, video games, and delivery of movies. It is widely used by the digital video, graphics, and moving image communities for both storage and transmission of digital moving images.

Recently the MPEG family acquired two new members, MPEG-7 and MPEG-21. MPEG-7, formally named “Multimedia Content Description Interface,” is a standard for describing the multimedia content data that supports some degree of interpretation of the information’s meaning, which can be passed onto, or accessed by, a device or a computer code. The audiovisual information described by MPEG-7 goes beyond the simple waveform or sample-based, compression-based (such as MPEG-1 and MPEG-2) or even objects-based (such as MPEG-4) representations, thus helping computer systems or humans to effectively use multimedia. MPEG-7 does not depend on the ways the described content is coded or stored. It is possible to create an MPEG-7 description of an analog movie or of a picture that is printed on paper, in the same way as digitized content. MPEG-7’s target readers contain both human users and automatic systems that process audiovisual information and so it covers both high-level areas of information such as creators and parental rating for humans and low-level areas of

information such as spatial, temporal or spatio-temporal structure of audiovisual content for computer programs.

The goal of MPEG-21 is defining the technology needed to support users to exchange, access, consume, trade, and otherwise manipulate digital items in an efficient, transparent and interoperable way. MPEG-21 aims at defining a normative open framework for multimedia delivery and consumption for use by all the players in the delivery and consumption chain. This open framework will provide content creators, producers, distributors, and service providers with equal opportunities in the MPEG-21-enabled open market. This will also be to the benefit of the content consumer providing them access to a large variety of content in an interoperable manner. The official MPEG web site is <http://chiariglione.org/mpeg/>.

MPEG audio is a subgroup of MPEG working on all audio aspects of the MPEG standards. The official website is <http://www.tnt.uni-hannover.de/project/mpeg/audio/>. Without data reduction, digital audio signals typically consist of 16-bit samples recorded at a sampling rate more than twice the actual audio bandwidth (e.g. 44.1 kHz for Compact Disks), or more than 1.400 Mbit to represent just one second of stereo music in CD quality. By using MPEG audio coding, you may shrink down the original sound data from a CD by a factor of 12, without losing sound quality. Using MPEG audio, one may achieve a typical data reduction of 1:12 by Layer 3 ([MPEG Audio Layer 3 \[MP3\]](#)), which corresponds with 112 kbps for a stereo signal, while still maintaining the original CD sound quality. For further information, please refer to <http://www.tnt.uni-hannover.de/project/mpeg/audio/faq/>.

*Required Standards:*

- ISO Information Technology -- Coding of Audio-Visual Objects, [ISO/IEC-11172](#), [ISO/IEC-13818](#) and [ISO/IEC-14496](#), [ISO/IEC JTC1/SC29/WG11](#), and [ISO/IEC JTC1/SC29/WG11/N5231](#).
- ISO MPEG Standards: [ISO/IEC-11172](#), [ISO/IEC-13818](#), [ISO/IEC-14496](#), [ISO/IEC JTC1/SC29/WG11](#), and [ISO/IEC JTC1/SC29/WG11/N5231](#).

**Table 4.7-28: MPEG Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.7-29: MPEG Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**Table 4.7-30: MPEG Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">RealNetworks</a>	RealOne	Player for multimedia material	x86-based workstation, MS Windows 2000, XP	AO

#### 4.7.14 Electronic Data Interchange

Electronic Data Interchange (EDI) is a standardized electronic method to facilitate the bidirectional electronic data file exchange in order to implement a specialized point-to-point interface between applications. EDI is used for application-to-application electronic exchange of business data. EDI provides a mechanism for the electronic exchange of data that traditionally is conveyed on paper documents. It is intended primarily for documents that are non-text (i.e., that consist of a sequence of numeric or alphanumeric fields).

EDI's cost makes it prohibitive for small to medium-sized organizations, while those able to afford EDI find that it locks them into data formats that are difficult to change and expensive to evolve. XML-based data descriptions now provide an alternative to EDI. XML's simplicity of design and the ability to describe data with tags has been a significant impetus to the creation of data vocabularies for 'Business to Business' e-commerce. Companies migrating to XML from EDI not only gain the advantage of basing their data descriptions on a globally recognized W3C standard, but also acquire the immediate ability to transport their data over the web using well-established globally recognizable protocols such as HTTP and Transmission Control Protocol/Internet Protocol (TCP/IP).

*Required Standards:*

- The PAN American (EDI for Administration, Commerce, and Transport) EDIFACT Board or United Nations Economic Commission for Europe for the EDIFACT family of EDI standards (The U.S. input to EDIFACT development is through the Pan American EDIFACT Board, one of the five EDIFACT boards.)
- The American National Standards Institute (ANSI) and the Data Interchange Standards Association (DISA) for the X12 family of EDI standards (this is for the U.S. implementation of EDI) <http://www.ietf.org/html.charters/ediint-charter.html>

**Table 4.7-31: EDI Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.7-32: EDI Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

The Judiciary has a couple of legacy EDI applications and custom codes its EDI mapping. EDI is included in the TRM because it is referenced by the MARC 21 Library interchange standard.

#### 4.7.15 Computer-Aided Design Data

Computer-Aided Design/Computer-Aided Manufacturing (CAD/CAM) files are used as a method of creating and storing complex engineering drawings in an electronic file format. The Institute for Global Environmental Strategies (IGES) standardizes the representation of specific types of complex graphic objects and attributes for data interchange. Product data interchange

encompasses technical drawings, documentation, and other data required for product design and manufacturing, including geometric and non-geometric data such as form features, tolerances, material properties, and surfaces. The information is typically associated with CAD/CAM data format exchange. IGES software consists of two processing modules: a pre-processor which transforms the native CAD system format into the neutral IGES format, and a post-processor that translates IGES format to the target system format.

*Required Standards:*

- ANSI Y14.26-1989; and IGES 5.2 (US PRO/IPO-100)

**Table 4.7-33: CAD Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Paladin Computing Solutions</a>	ARRIS V 7.08	Architecture Drawings	Unix	AO
<a href="#">Autodesk</a>	AutoCAD V 14	Network Drawings	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO
<a href="#">Microsoft</a>	Visio	Space Planning	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO

**Table 4.7-34: CAD Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

#### 4.8 Graphics Services

Graphics Services provide interfaces for programming two- and three-dimensional graphics in a device-independent manner. Graphics Services are implemented through Graphical Kernel System (GKS) functionality. GKS defines library calls for virtually any kind of two-dimensional graphic image. It provides interfaces to two-dimensional graphical objects to be displayed or plotted on raster or vector graphics devices.

*Required Standards:*

- ISO/IEC 8651-4:1991: Information Processing Systems – Computer Graphics -- Graphical Kernel System (GKS) Language Bindings
- ANSI INCITS 124-1985 (R2002): Graphical Kernel System (GKS) Functional Description (includes ANSI X3.124.1-1985) (formerly ANSI Standard X3.124-1985 [R1996])
- ISO 7942:1985: Information Technology – Computer Graphics and Image Processing - Graphical Kernel System (GKS)

- INCITS/ISO/IEC 8632-1-1999: Computer Graphics – Metafile for the Storage and Transfer of Picture Description Information - Part 1: Functional Specification
- INCITS/ISO/IEC 8632-3-1999: Computer Graphics – Metafile for the Storage and Transfer of Picture Description Information- Part 3: Binary Encoding
- INCITS/ISO/IEC 8632-4-1999: Computer Graphics – Metafile for the Storage and Transfer of Picture Description Information - Part 4: Clear Text Encoding

**Table 4.8-1: Graphics Services Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Microsoft</a>	MS Visio	Graphics, charts	x86-based workstation MS Windows 95, 98, ME, NT, 2000	

**Table 4.8-2: Graphics Services Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.9 Computer-Based Interactive Training

Computer-based interactive training is a cost-effective way of providing training to users. This type of training can be taken whenever a user needs it versus having to wait for a class to be held. The material can also be used as a reference when only a particular topic is unknown or needs to be refreshed by the user.

**Table 4.9-1: Computer-Based Interactive Training Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
		Graphics, charts	x86-based workstation MS Windows 95, 98, ME, NT, 2000	

**Table 4.9-2: Computer-Based Interactive Training Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**Table 4.9-3: Computer-Based Interactive Training Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Macromedia</a>	Authorware 7.0	Authoring tool	x86-based workstation, MS Windows 2000, XP	AO
<a href="#">Asymetrix</a>	ToolBook Instructor	Authoring tool	x86-based workstation, MS Windows 2000, XP	AO

## 4.10 Output Services

Output services provide common software access to the external environment output device hardware across the Judiciary information infrastructure. Generic output services enable the results of application processing to be distributed by formatting and generating the data to be output in a variety of character-based, raster-based or graphics-based products for distribution on a variety of media. These include:

- Facsimile Transmission Service (fax)
- Compact Disk-Read Only (CD-ROM) Generation Service
- Digital Versatile Disc (DVD) Generation Service
- Digital Video and Film Generation Service
- Magnetic Tape Generation Service
- Plotting Service
- Print Service

### 4.10.1 Facsimile Transmission Service (fax)

Facsimile transmission services provides a way for output of applications to be sent directly to a fax machine without having to print out and manually use a fax machine.

*Required Standards:* N/A

**Table 4.10-1: Facsimile Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.10-2: Facsimile Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**Table 4.10-3: Facsimile Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
<a href="#">Captaris</a>	RightFax	Computer based faxing		AO

### 4.10.2 Compact Disk-Read Only (CD-ROM) Generation Service

CD-ROM manufacturers and CD-ROM drive software providers use standard specifications for creation of compact disk read-only (CD-ROM) and compact disk (CD) recordable media. CD-ROM is one medium of choice for dissemination of custom products; an application requiring this service is one that will initiate a CD-ROM to be mastered and subsequently replicated for distribution to the public or internally.

ISO 9660 is the universal standard defining the preferred volume and file structure for all CD-ROM authored disks. It is used across a variety of processing platforms. Virtually all CD-ROM

manufacturers and CD-ROM drive software providers use ISO 9660 as the file system for organizing and locating file and directories on CDs.

*Required Standards:*

- CD-ROM Volume/File Structure ISO/IEC ISO 9660:1988
- Refer to Electronic Data Interchange Standard section 4.7.14

**Table 4.10-4: CD-ROM Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.10-5: CD-ROM Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

### 4.10.3 Digital Versatile Disc (DVD) Generation Service

DVD services are provided by software used to manage video, audio, linguistic, text, and other resources that are combined into a DVD product. The software may be used to develop a timeline, to associate various files with events on the timeline, create menus and associated program actions, and perform MPEG compression on the video files. After the content is fully “authored”, the DVD service software is used to create a DVD disc image, and execute testing using simulation.

There are several DVD formats such as DVD-video, DVD-audio, DVD-R (write-once, read-many), DVD-RAM, and DVD-ROM. DVD-ROM is a read-only format of DVD that was designed as an optical storage media for imaging. It is an evolutionary technology that picks up where CD-ROM leaves off. Physically, DVD discs have the same 5 ¼-inch footprint used in CD-ROMs. DVD discs, however, are loaded much more densely with data, and storage capacities start at 4.7 Gbytes. This is enough capacity to store the data from seven CD-ROMs, or an average-length motion picture. The DVD-ROM functional intent is to bring theater-quality video and surround sound to PCs. Second-generation DVD-2 products are able to read CD-Recordable or CD-Rewritable media although they do not match the performance speeds of some CD-ROM drives. While current discs hold 4.7 Gbytes of data on a side, future DVD-ROM media will store data on both sides and employ dual-layer media to store 17 Gbytes of data. To exploit the multimedia capabilities of most DVD titles fully, additional hardware (decoder card with MPEG-2, AC-3, and CSS chips) is usually required.

DVD Authoring and Emulation Tools: Advanced authoring software provides the tools to author, format, and emulate the production of DVD title. Basic features include DVD Video 1.0, MPEG2 still-frame encoding from TIFF, and BMP 24-bit graphic files, as well as a professional-level DVD emulator and debugging tools, DVD formatting, and layout.

*Required Standards:* Emerging standard.

- DVD Version 1.0, 1991. Developed by the DVD Forum, which consists of 17 industry steering committee members and 220 members.
- DVD File system based on ISO 13346, subset of Universal Disk Format (UDF).
- ISO 4660, UDF Bridge.
- Refer to Electronic Data Interchange Standard section 4.7.14

**Table 4.10-6: DVD Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Roxio</a>	CD Creator	Creating CD and DVD	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">Nero</a>	Nero	Creating CD and DVD	x86-based workstation, MS Windows 95, 98, ME, NT, 2000, XP	

**Table 4.10-7: DVD Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

#### 4.10.4 Digital Video and Film Generation Service

*Required Standards:*

- ISO/IEC 13818-2:2000: Information Technology – generic coding of moving pictures and associated audio information; video; parts.

**Table 4.10-8: Digital Video Generation Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.10-9: Digital Video Generation Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

#### 4.10.5 Magnetic Tape Generation Service

Magnetic tape is a common medium for disseminating large volumes of data. For example, an application using this capability might retrieve selected documents from a judiciary database and copy them to magnetic tape. A Magnetic Tape Generation Service provides a common set of

functions under a consistent API that applications employ to perform a tape generation operation. In addition to data recording, the services include cataloging, labeling, logistics and related administrative functions.

With the large size of data collections, backups no longer fit on a single tape. Tape libraries are frequently needed to manage the large sets of tapes needed to provide appropriate backup storage. Smaller libraries can be controlled by simple commands such as “load the next tape in sequence”. Larger tape libraries need software to control and manage the many tapes and, possibly, many tape drives in the library. Since there are no standards for tape libraries it is critical to check with the vendors of both the tape library and the controlling software for compatibility.

*Required Standards:*

- ANSI NCITS 311-1998: Information Technology – Magnetic Tape Format for Information Interchange
- ANSI NCITS 312-1998: Information Technology – Magnetic Tape Format for Information Interchange, DLT4 Format
- ANSI NCITS 315-1998: Information Technology – Magnetic Tape Format for Information Interchange, DLT4 Format
- ANSI NCITS 334-2000: Information Technology – Magnetic Tape Format for Information Interchange, DLT-3-XT Format
- ANSI NCITS 341-2000: Digital Cartridge Tape Format
- ANSI NCITS 345-2000: Magnetic Tape Cartridge for Information exchange
- ANSI NCITS 329-2000: DLT5 Format
- Linear Tape-Open (LTO)  
<http://www.lto-technology.com/newsite/index.html>

**Table 4.10-10: Magnetic Tape Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Dell</a>	DLT7000	Backup Device	x86-based server, MS Windows NT	DOM <sup>1</sup>
<a href="#">Exabyte</a>	Mammoth-2	Backup Device	x86-based server, Solaris 7	ALL
<a href="#">Exabyte</a>	Mammoth 8900LVD	Backup Device	x86-based server, Solaris 7	ALL
<a href="#">Exabyte</a>	Eliant 820	Backup Device	x86-based server, MS Windows 2000	PCT <sup>2</sup>

**Table 4.10-11: Magnetic Tape Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Tape Library	x86-based server, Linux	ALL

<sup>1</sup> DOM: E-Mail server backup medium

<sup>2</sup> PCT: PACTS Report Server

**Table 4.10-12: Magnetic Tape Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
HP	LTO	Backup Device	x86-based server, Linux	ALL

#### 4.10.6 Plotting Service

Plotting is a specialized output function that produces graphical data from a variety of graphical generators. Examples of the graphical data are network diagrams, facilities diagrams, mechanical drawings, maps, and scientific charts. Plotting is distinguished from printing in that plotters typically accommodate larger size drawings, e.g., E-size, have continuous form paper, and draw line segments instead of generating raster dots. The plotting service provides a common set of functions and a corresponding API to enable projects to invoke standard plotting functions and facilities in a consistent manner. Functions include paper setup, pen/color configurations, scrolling, and job identification and control.

**Table 4.10-13: Plotting Service Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
HP	HP Designjet 1055am Plus	Plotter		

**Table 4.10-14: Plotting Service Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.10.7 Print Service

Print Service supports the printing of documents, files, or other printable entities through a common and consistent set of functions and API. These functions include such operations as print job description, job submission, priority assignment, and status query. By standardizing on a common print service, Judiciary units can make use of shared infrastructure components and operate with new print technologies without major redesign.

The ISO DPA 10175 standard addresses those aspects of document processing that enable users in a distributed open systems environment to send electronic documents to be shared and printed on geographically dispersed printers in accordance with user preferences. The DPA 10175 standard focuses on the final phase of the document processing cycle, i.e., the queuing, preparation, rendering, and finishing of the fully composed form of the document on the final destination. The DPA 10175 standard defines the objects needed to make this happen and the interaction between them. This includes object classes, operations, attribute types, and attribute values.

The POSIX 1387.4 standard builds on the ISO DPA 10175 standard to define programmatic and user interfaces for a printing system that can be used in both local and distributed environments. This includes an application program interface (API), a command line interface (CLI), and a set

of managed objects. The CLI provides common utility programs for use by application programs (including shell scripts) and humans. A managed object provides a foundation for the definition and implementation of printing system functionality and interoperability.

*Required Standards:*

- ISO DPA 10175–1:1996:: Document Printing Applications
- POSIX 1387.4: Printing Interfaces
- CCITT Group 4 Raster Image

**Table 4.10-15: Print Service Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Novell</a>	<a href="#">Novell Distributed Print Services</a>	Network print management	x86 server, Novell NetWare	

(Network print services are covered in Section 4.11.4.)

**Table 4.10-16: Print Service Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

**Table 4.10-17: Print Service Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Open Source	SAMBA	Network print services	x86-based server	

**4.11 Network Services**

The network services infrastructure allows judiciary personnel to effectively share electronic information. Standard protocols and COTS equipment are used to facilitate data exchange between court personnel. Local data communication equipment and software combine to create Local-Area Networks (LANs) that link computer equipment within an office or building. Wide-Area Network (WAN) communication services are currently provided by the Judiciary’s Data Communications Network (DCN) for interoffice or building connectivity.

The communication infrastructure is designed in the context of four functional objectives:

- **Connectivity** – The communication infrastructure must support the interface to current and anticipated processing equipment within the judiciary.
- **Interoperability** – The communication infrastructure must provide mechanisms to permit hardware from competing vendors to communicate, and implement an open system design that allows system independence and flexibility.
- **Scalability** – The communication infrastructure must be configurable to support the required range of user community sizes, traffic requirements, and site-unique topologies.

In this context, scalability is synonymous with a system design which is adaptable to present demands and future uses.

- Security – The communication infrastructure must provide mechanisms to insure the privacy of information transmitted on the networks, security of systems connected to the networks and the integrity of data accessible on the networks.

Networks and their services are commonly characterized as traditional LANs, WANs, Intranet, and the Internet. Internal networks have traditionally supported centralized and distributed applications, including client-server functional applications, office automation product use, and shared data files and resources such as printers. Internal network access is secured through user authentication and physical connectivity limitations. A LAN is generally defined as a privately owned data communications system and usually covers a limited territory, hence the term “local area.”

As the geographical scope of the network grows by connecting users in different cities or different states, LANs grow into a WAN. The judiciary’s WAN is based on frame relay which provides one or more T-1 (1.544 Mbps) lines to each site. There are two gateways for the Judiciary to the Internet with T-3 (45 Mbps) connections.

The public Internet is an Internet Protocol (IP)-based network provided by a collaborative international group of service providers which adhere to de facto network protocols and standards (e.g., TCP/IP). Primary Internet Service Providers (ISPs) form the core of the public Internet. Individuals, businesses, and institutions access the public Internet to exchange information and access services. The public connection to the Internet is accomplished through public telecommunications systems (e.g., telephone lines, integrated services digital network [ISDN], cable, LAN/WAN etc.). Internet web sites normally link to the Internet for public to access through a WAN link such as a T-1 line. In general, public web sites require no access control or authentication. However, they may be behind a firewall that only allows certain types of traffic to go through (e.g., HTTP traffic only).

Intranets are essentially IP-based networks that can support internal Web sites for use by employees, not the general public. Intranets are characterized as fairly secure, and protected by a firewall system designed to prevent external access. The Intranet organization-owned information is generally accessible only to those physically located at the organization facility, or through secured connections. For example, <http://jnet.ao.dcn/> is an Intranet web site at the Judiciary that enables the sharing of information and computing resources available behind the firewall and only among employees.

Extranets are private IP-based networks that allow authorized third-party access. Extranets are normally accessed through private network connections (e.g., frame relay or T-1 lines) or through public telecommunications combined with virtual private network (VPN) technologies. The Judiciary network infrastructure is described in the following sub-sections:

- National Internet Gateway
- DCN/Backbone Configuration
- PacerNet

- Network File and Print Services
- Directory and Naming Services
- Domain Name Service (DNS)
- Electronic Mail, Message Services
- Time Services

#### 4.11.1 National Internet Gateways

Computers on the courts' LANs gain access to the Internet through one of two national Internet gateways. Desktop systems can then access Internet resources, provided they have the applications that supply the TCP/IP protocols. The gateways connect to the Internet at T-3 speeds. Access to a court's LAN from outside the court via Internet is controlled by dedicated servers designed to isolate access through firewall protection providing access from the internal network to the unsecured external network. Access to court information can be made available through World Wide Web (WWW) servers.

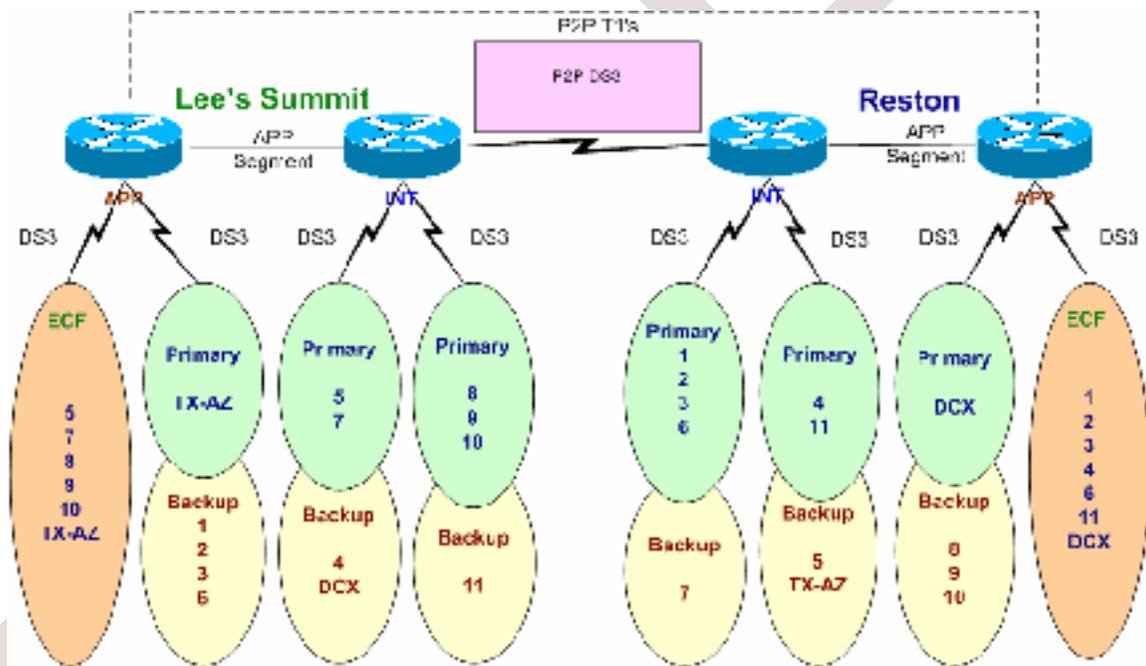


Figure 4.11-1: Two National Gateways Service Areas

Table 4.11-1: National Internet Gateway Products Used by the Judiciary

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T-1/T-3	Internet Gateway	DCN WAN	ALL
<a href="#">Cisco</a>	Routers	Internet Gateway	Cisco switches, routers	ALL

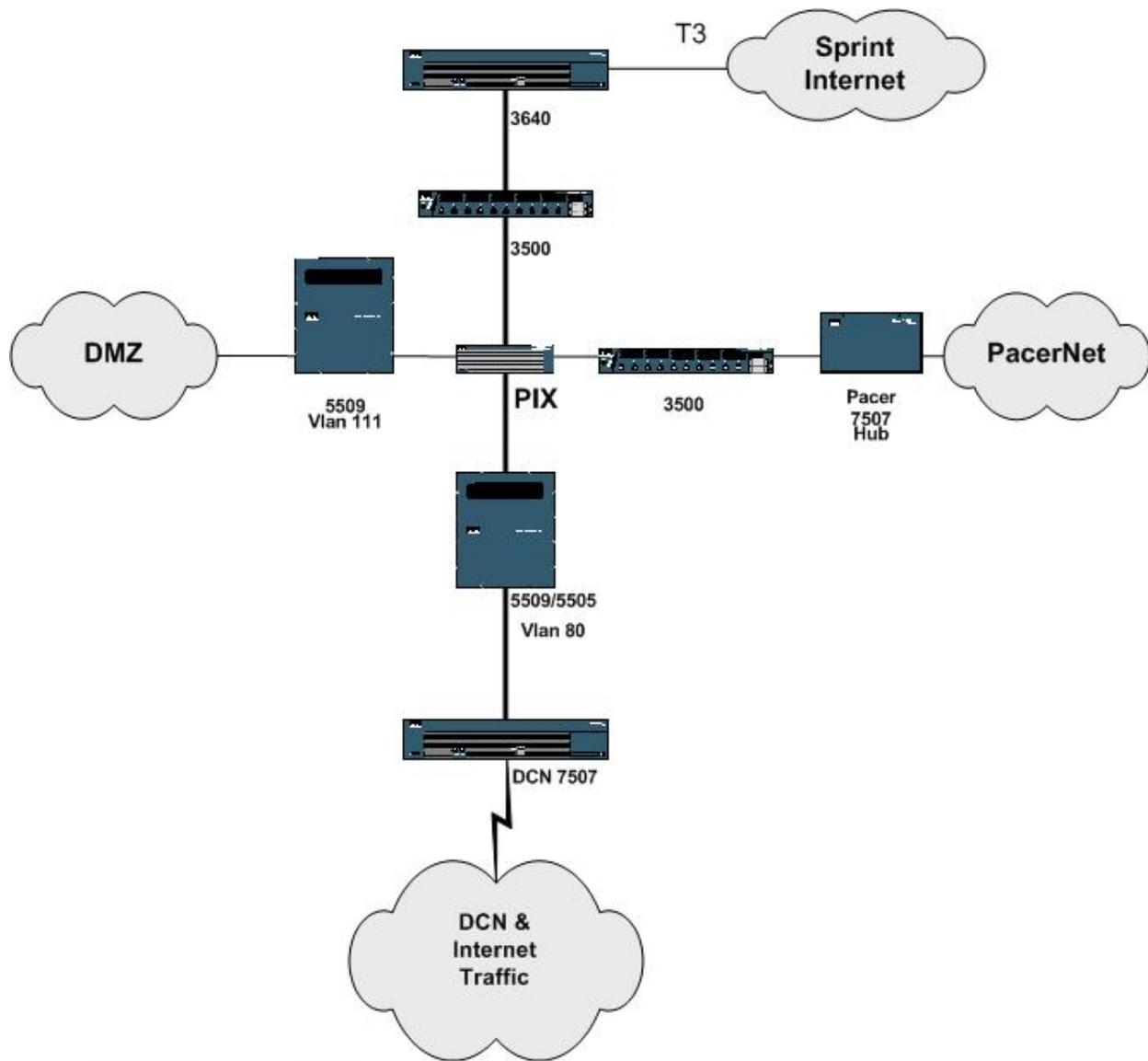
Table 4.11-2: National Internet Gateway Preferred Product for the Judiciary

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T-1/T-3	Internet Gateway	DCN WAN	ALL

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T-1/T-3	Internet Gateway	DCN WAN	ALL
<a href="#">Cisco</a>	Routers	Internet Gateway	Cisco switches, routers	ALL

#### 4.11.2 DCN/Backbone Configuration

WAN access is provided by the DCN. FTS 2001 Managed Frame Relay Service access lines and permanent virtual circuits (PVCs) provide a partially meshed network. This meshed network allows an upstream node to fail and still allow downstream nodes connectivity to the DCN through the Internet gateway PVC. All court divisional offices have at least one T-1 access line and PVCs to the Internet and legal research gateways, and their upstream headquarters site, and the site that hosts the Lotus Notes e-mail server. All court headquarters' sites have at least one T-1 access line, the PVCs mentioned above, and additional PVCs to the circuit hub and AO hub. All circuit hubs have high-speed connections with a primary PVC to the Internet Gateway, a backup PVC to an alternate Internet Gateway, and a primary PVC to the AO Hub. A mix of multiple T-1s or T-3s is used at the circuit hubs depending on the total traffic flow volume.



**Figure 4.11-2: National Gateway for DCN, PacerNet, and Network Services**

**Table 4.11-3: DCN Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T-1/T-3	DCN WAN	DCN WAN	ALL
<a href="#">Cisco</a>	Routers	DCN WAN	Cisco switches, routers	ALL

**Table 4.11-4: DCN Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T-1/T-3	DCN WAN	DCN WAN	ALL
<a href="#">Cisco</a>	Routers	DCN WAN	Cisco switches, routers	ALL

### 4.11.3 PacerNet

The Public Access Network (PacerNet) is a Virtual Private Network (VPN), configured separately from the DCN, that operates over an existing telecommunications network administered and is managed by US Sprint. The public connects with one of the national gateways, enters a separate public access gateway, and is then routed over the virtual private network to the court's public access computer, containing the requested data. The Judiciary's private network (DCN) remains insulated from public use, and access points are controlled and subject to security standards. PacerNet currently supports over 160 sites and more than 1,000 web servers.

The primary advantages of this approach are: (1) the DCN can continue to accommodate judiciary traffic only, avoiding the possible necessity for costly bandwidth upgrades; (2) a separate public access network reduces the security concerns because public traffic does not enter the DCN; (3) users are able to access multiple court sites without having to disconnect a session and dial a new court; (4) the courts have the ability to enhance the Public Access to Electronic Court Records (PACER) products with locally and vendor-developed systems, local information, and home pages; and (5) PacerNet uses state-of-the-market technology that will be easier for the public to use and for the courts to use for local initiatives.

PacerNet allows connections via one of two Public Access Network Internet access points through a Private Internet Exchange (PIX) firewall. The PIX firewall is configured to allow only HTTP, HTTPS, and FTP (ports 80, 443, and 20/21 respectively) connections initiated from the Internet. No other connections from the Internet are permitted. There are no connections available that would allow traffic to the Internet which was initiated from inside PacerNet.

The PIX firewall is connected via an Ethernet connection to a frame relay access device (FRAD). The FRAD is connected to the frame relay network (also called a frame relay "cloud") by a trunk line that consolidates all the PVCs that terminate at that site. The trunk line is sized to handle the aggregate traffic of the site which is typically the same size as the Internet access connection. The FRAD and the connection to the frame relay cloud are managed by the frame relay provider. The other end of the PVC is terminated by a FRAD at the court. Again, the FRAD and the connection to the frame relay cloud is managed by the frame relay provider. The court's FRAD is connected to an Ethernet Hub (or switch). The Ethernet Hub is also connected to the PACER box and to one Ethernet port on the DCN router for the building. The PacerNet connection only allows Web support to the authorized servers such as the Pacer box. The PACER box, itself, continues to support dial-in access via modems.

The DCN router is configured to perform Network Address Translation (NAT) and enforce access control lists (ACLs) for the Ethernet port connected to the PacerNet Ethernet hub. The net result is that the DCN router functions like a firewall and isolates PacerNet activity from both the DCN and the building router, which is connected to the LAN or building network. The DCN router is configured to allow passive FTP, HTTP, HTTPS, UUCP, Netbios, and Telnet connections originating from the DCN or the building router. No connections originating from the PACER box or PacerNet are allowed. IP addresses on PacerNet are valid only on PacerNet. PacerNet IP addresses are converted to valid DCN IP addresses by the DCN router if routing is permitted. The DCN router is under the control of the DCN management. The PACER box is under the control of the court.

**The PacerNet architecture consists of the following key features:**

- **A two-gateway architecture**, whose locations currently serve as Internet connections for U.S. Courts staff access. The data path for public access is kept totally separate from the data path for staff access at the gateway sites. Each public access gateway has high-speed (T-3 [45Mbps]) access to the ISP. The ISP service is brought into a Cisco PIX firewall which filters the access to PacerNet. This filtering is described later in the section.
- **A frame relay network** is provided by US Sprint under the FTS-2001 contract. The frame relay network interconnects the gateway sites with the prototype PACER servers at selected court sites. The routers used on this network have been leased from, and are managed by, the FTS-2001 contractor. The gateway sites use a Cisco 7500 router, while the courts use a Cisco 2501.
- **PacerNet Web servers** for U.S. Bankruptcy courts and District courts consist of several variations. CM/ECF includes PACER functionality and will eventually replace almost all public access network web servers. Software has been developed which allows registered PACER users to log in and be billed for usage on a per-page basis. These servers utilize a Secure Sockets Layer (SSL) version of the Apache (Stronghold) for secure login. Along with Appellate, District, and Bankruptcy versions of PACER, other Web servers which will appear on PacerNet until they are replaced by CM/ECF include the National Integrated Bankruptcy System (NIBS) public access systems, commercially available systems such as Wade Systems (RACER), WebPACER (Public Access to Court Electronic Records), an application for courts with Integrated Case Management Systems (ICMS), and imaging systems developed by the courts.

**Table 4.11-5: PacerNet Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T-1/T-3	PacerNet	DCN WAN	ALL
<a href="#">Cisco</a>	Routers	PacerNet	Cisco switches, routers	ALL

**Table 4.11-6: PacerNet Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T-1/T-3	PacerNet	DCN WAN	ALL
<a href="#">Cisco</a>	Routers	PacerNet	Cisco switches, routers	ALL

**4.11.4 Network File and Print Services**

Network Operating Systems (NOSs) provide networked file and print services. Network file services provide transparent access to files and file systems without regard to location. Transparent access allows applications to access remote files as if they are part of the local file system.

File Transfer Services support copy, replication, and moving whole files across a network. FTP is an industry-prevalent mechanism found in most TCP/IP implementations. Files can also be transferred via e-mail. Section 4.11.7, Electronic Mail and Message Services, provides further

information and standards for Simple Mail Transfer Protocol (SMTP) and Internet Mail Protocol. Section 4.15.10 provides standards and references for Multipurpose Internet Mail Extensions (MIME). Print Services support the printing of documents, files or other printable entities through a common and consistent set of functions and API.

In general, files are stored on storage devices that are attached to a single file server. Relatively recent technologies such as Storage Area Network (SAN) and Network Attached Storage (NAS) have appeared to provide server-independent storage of files on the network. Within the Judiciary, there are a variety of operating systems that are capable of providing NOS capabilities. Many of the NOS servers are Novell NetWare, but there are also Microsoft NT 4.0, Windows 2000, and Linux servers used as the NOS for file and print (in addition to being used as application servers).

On the UNIX platform, the Network File System (NFS) from Sun Microsystems, and Distributed File Service (DFS) from The Open Group (TOG) have been used to access network information. Both NFS and TOG adhere to POSIX 1003.1 standard; deviations are addressed in POSIX 1003.8.

*Required Standards:*

- POSIX 1003.1 standard
- POSIX 1003.8 Transparent File access specification
- RFC 959 File Transfer Protocol (FTP)  
<http://www.w3.org/Protocols/RelevantProtocols.html>  
<http://www.rfc-editor.org/rfcxx00.html#STDbRFC>
- ISO 8571 File Transfer, Access and Management, Information Systems --- Open Systems Interconnection --- File Transfer, Access and Management.  
[http://www.iso.ch/iso/en/Standards\\_Search.StandardsQueryForm](http://www.iso.ch/iso/en/Standards_Search.StandardsQueryForm)

**Table 4.11-7: NOS Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
OS Vendor	FTP Server	File Transfer Service	x86-based server	ALL
Open Source	SSH	File services	x86-based server	ALL
Open Source	Samba	File and print services	x86-based server	ALL
<a href="#">Cisco</a>	TFTP	Trivial FTP service	Cisco switches, routers	ALL
<a href="#">Microsoft</a>	NT/2000 Server	File and print services	x86-based Windows NT/2000 server	Local
<a href="#">Novell</a>	NetWare	File and print services	x86-based Novell NetWare Server	Local
<a href="#">Novell</a>	LAN Workplace	File Transfer Service	x86-based workstation	ALL
<a href="#">Sun</a>	Solaris	Network File System (NFS) and DNS server(s)	RISC-based UNIX	ALL

Refer to <http://serverwatch.internet.com/ftpservers.html> for a list and short review of ftp server products.

**Table 4.11-8: NOS Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Open Source	SSH	File services	x86-based server	ALL

**Table 4.11-9: NOS Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Open Source	SAMBA	Network print services	x86-based server	

#### 4.11.5 Directory and Naming Services

Directory and naming services provide means for locating objects or resources on the network. A directory service is a repository of information concerning what is available on the network, who is authorized to access the network, and which resources are accessible to each authorized user. A directory service is a database in which each object is identified by its attributes, where one of the attributes is its name. A naming service locates and retrieves information about an object solely by the name of the object. There are stand-alone systems such as the Domain Name Server (DNS) that implement a naming service. Most are integrated with other services, such as file systems and e-mail.

An enterprise directory helps people find destination recipients in other organizations. The Judiciary uses the directory within Lotus Domino for its national directory. Applications outside of Lotus Domino can access this directory by its Lightweight Directory Access Protocol (LDAP) interface. LDAP standardizes a directory access protocol that allows applications or other services to access multiple LDAP-compliant directories if the directories share common naming standards and field formats.

In the context of a computer network, a directory (also called a data store) is a hierarchical structure that stores information about objects on the network. Objects include shared resources such as servers, shared volumes, and printers; network user and computer accounts; applications, services, security policies, and just about everything else in the network. An example of the type of information a network directory might store about an object is the name, password, e-mail address, phone number, and so on, for a user account.

A directory service differs from a directory in that it is both the directory information source and the service making the information available and usable to administrators, users, network services, and applications. Ideally, a directory service makes the physical network topology and protocols (formats for transmitting data between two devices) transparent so that a user can access any resource without knowing where or how it is physically connected. To continue the user account example, it is the directory service that lets other authorized users on the same network access stored directory information (such as an e-mail address) about the user account object.

Directory services can support a wide variety of capabilities. Some directory services are integrated with an operating system, and others are application specific, such as e-mail directories. Network Operating System directory services, such as Novell Directory Services (NDS) and Microsoft's Active Directory (AD), manage users, computers, and shared resources. E-mail directory services, such as Lotus Notes, enable users to look up other users and send e-mail.

X.500 is set of international standard protocols that provide the directory services interoperability among heterogeneous computer systems. It was designed to enable an enterprise-wide distributed naming and directory service for any kind of information. X.500 is thought of as a general purpose repository of all kinds of information. The directory information could include the names of users and organizations, network and mailbox addresses, and message distribution lists. X.500 allows applications on one system to locate and retrieve information about resources on another system. Its most important role in the near future is as an enabling technology for data communications, especially network objects, electronic messaging, and workgroup applications. The framework of X.500 is as follows:

- C = Country Name
- O = Organization Name
- OU = Organizational Unit Name
- CN = Common Name for other objects in the Directory Information Tree (DIT)

X.500 is an overall model for Directory Services in the broader Open System Interconnection (OSI) model. The X.500 model encompasses the overall namespace and the protocol for querying and updating it. The protocol is known as Directory Access Protocol (DAP). DAP runs over the OSI network protocol stack. The OSI network protocol stack combined with X.500's very rich data model and operation set makes it quite a heavyweight. There is rarely a full-blown DAP client implemented on small computer systems.

LDAP is a subset of X.500 DAP without the overhead of ASN.1 or the OSI protocol stack. LDAP is, like X.500, both an information model and a protocol for querying and manipulating it. LDAP's overall data and namespace model is essentially that of X.500. The major difference is that the LDAP protocol itself is designed to run directly over the TCP/IP stack, and it lacks certain DAP protocol functions. LDAP was originally intended as a means for clients on PCs to access X.500 directories, but can also be used with any other directory system which follows the X.500 data models. The current version is LDAPv3, which was ratified in December 1997.

The LDAPv3 core specifications contain the following:

- Protocol specification
- Attribute syntax definitions
- String representation of search filters
- LDAP URL format
- X.500 (96) schema definitions

LDAPv3 improves compatibility with X.500 and also better specifies how LDAP can be used with non-X.500 and standalone directories. For further information refer to

<http://www.kingsmountain.com/ldapRoadmap.shtml#Introduction>

*Required Standards:*

- LDAP v2, v3. LDAPv3, is an update developed in the Internet Engineering Task Force (IETF), which address the limitations found during deployment of the previous version of LDAP, RFC 1779  
<http://www.ietf.org/rfc.html> or [http://www.ietf.org/iesg/lrfc\\_index.txt](http://www.ietf.org/iesg/lrfc_index.txt).

MetaDirectory products provide multidirectional synchronization between user repositories (i.e., Novell’s eDirectory and Microsoft’s Active Directory) and provide a unified view of the information they are synchronizing. A metadirectory server can synchronize directories and user repositories and enforce security rules and policies as part of the synchronization process. For example, an automated synchronization solution can ensure that login names are properly formatted and user names are in a consistent (or, at least, predictable) format.

**Table 4.11-10: Directory Service Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Novell</a>	Novell Directory Service (NDS)	Directory Services	Novell NetWare server	Local
<a href="#">Novell</a>	NDS for NT	Directory Services	Windows NT / 2000 Server	Local
<a href="#">Microsoft</a>	Active Directory – Windows 2000	Directory Services	Windows 2000 Server	Local
<a href="#">IBM/Lotus Development Corp.</a>	Domino	E-mail directory	Notes Server	ALL

**Table 4.11-11: Directory Service Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">IBM</a>	Directory server	National directory	Mainframe, x86-based server, Linux	ALL

**Table 4.11-12: Directory Service Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
		Enterprise LDAP server	x86-based server	ALL

#### 4.11.6 Domain Name Service

TCP/IP uses four-byte numbers that uniquely identify a computer or device on an internetwork. The IP address format is nnn.nnn.nnn.nnn. Routers and switches each have similar addresses. For one machine or device to communicate with another, each must know the other’s IP address. Most people find it difficult to remember such numeric addresses and work much more easily with descriptive names (for example, “[www.uscourts.gov](http://www.uscourts.gov)”). In the early stages of the Internet, host files on the local machine were used to resolve descriptive host names to numeric IP addresses. As the number of connected machines / devices grew, this rapidly became unmanageable. Domain Name Service (DNS) servers are the solution to this problem in a large, distributed, environment. Each machine or device is now configured to reference a DNS server.

Each machine name and domain name is mapped to a particular IP address in a DNS server. When a name is invoked, a DNS server is queried and performs the name-to-address mapping. DNS servers are implemented in a hierarchy, each referencing a higher level up to the .gov, .com, .net, .org, and .edu suffixes. Thus every registered host name on the Internet is resolvable to a numeric IP address.

Host names are used to manage network resources including routers, concentrators, and switches and are all in the Judiciary's DNS. Domain names are part of the machine name used in e-mail addresses and in host names. This scheme enables users to invoke an easy-to-remember name instead of a string of numbers when using the Internet.

*Required Standard:*

- RFC 1034, Domain Names—Concepts and Facilities
- RFC 1035, Domain Names—Implementation and Specification
- RFC 1996, addendum to RFC 1035
- RFC 2308 March 1998, update RFC 1034 and RFC 1035  
<http://www.rfc-editor.org/rfcxx00.html#STDbyRFC>

**Table 4.11-13: DNS Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
OS Vendor	Bind	DNS server	x86-based server	ALL
<a href="#">Sun</a>	Solaris	DNS server	RISC-based UNIX	ALL

**Table 4.11-14: DNS Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
OS Vendor	Bind	DNS server	x86-based server	ALL

**4.11.7 Electronic Mail and Message Services**

Electronic mail and message services provide Judiciary employees the ability to communicate both within and outside of the boundaries of the Judiciary. The Judiciary's internal mail system is Lotus Notes. The mail system includes two major components, the Enterprise Mail gateway System (EMS) and the Internal Mail System. The EMS receives and examines the mail to and from the Internet to the internal mail system and provides virus scans (reference section 4.16.4.4- Virus Control). The internal mail system receives e-mails and distributes them to appropriate mail boxes and permits users to access their e-mails at their designated mail servers. Instant messaging and web conferencing is handled by the Lotus Sametime product.

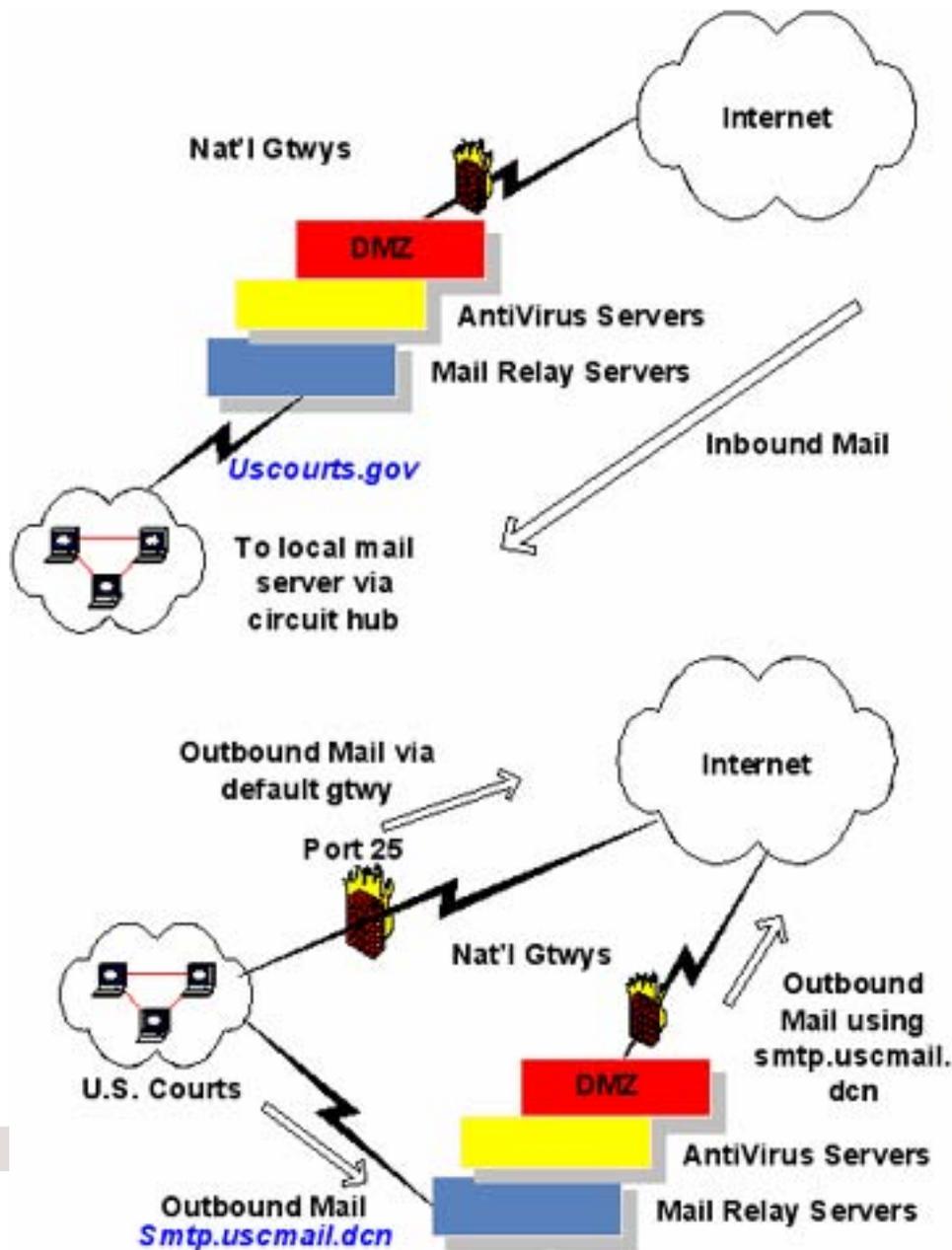


Figure 4.11-3: National E-Mail Gateway

Electronic mail and message services are based on several protocols and standards, including:

- RFC 2045 Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
- Lightweight Directory Access Protocol (LDAP) for authentication and address book access
- Simple Mail Transport Protocol (SMTP) for Internet message transmission

- Post Office Protocol 3 (POP3) for standard mailbox access
- Internet Message Access Protocol (IMAP) for server-side mailbox access
- MIME for standard transmission of non-text file attachments.
- S/MIME MIME with Rivest, Shamir, Adleman (RSA) encryption for strong e-mail security.

*Required Standards:*

- RFC 2045 MIME - Multipurpose Internet Mail Extension
- [RFC 2633](#), RFC 2632, RFC 2634 S/MIME Secure/Multipurpose Internet Mail Extensions
- RFC2060 IMAP Internet Message Access Protocol - Version 4rev1
- RFC821 SMTP Simple Mail Transfer Protocol

For further information, refer to <http://www.rfc-editor.org/rfcxx00.html#STDbRFC> and search for these terms.

**Table 4.11-15: E-mail and Messaging Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Sendmail</a>	Sendmail	Internet E-mail gateway	x86-based server	ALL
<a href="#">IBM/Lotus Development Corp</a>	Notes	Internal Mail	x86-based server	ALL
<a href="#">IBM/Lotus Development Corp</a>	Sametime	Instant Messaging/ Web Conferencing	x86-based server	ALL

**Table 4.11-16: E-mail and Messaging Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Sendmail</a>	Sendmail	Internet E-mail gateway	x86-based server	ALL
<a href="#">IBM/Lotus Development Corp</a>	Notes	Internal Mail	x86-based server	ALL
<a href="#">IBM/Lotus Development Corp</a>	Sametime	Instant Messaging/ Web Conferencing	x86-based server	ALL

#### 4.11.8 Time Services

Time services are established to ensure consistency and accuracy of time and dates across distributed systems. Network Time Protocol (RF1305) is a simple method of obtaining time across a network.

The Network Time Protocol (NTP) is a protocol for synchronizing a set of network clocks using a set of distributed clients and servers. NTP is built on the User Datagram Protocol (UDP), which provides a connectionless transport mechanism. It is derived from the Time Protocol and the Internet Control Message Protocol (ICMP) Timestamp message. NTP has replaced both.

*Required Standard:*

- RFC 1305, NTPV3 – Network Time Protocol (Version 3) Specification, Implementation

**Table 4.11-17: Time Service Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	Cisco IOS	Time service	Cisco	ALL
<a href="#">Microsoft</a>	Windows Time Server	Time service	x86-based Windows NT/2000 server	Local
<a href="#">Novell</a>	NetWare	Time service	x86-based Novell NetWare Server	Local
<a href="#">Sun Microsystems</a>	Solaris	Time service	Sun Sparc	ALL

**Table 4.11-18: Time Service Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Cisco	Cisco IOS	Time service	Cisco router	ALL

## 4.12 Videoconferencing

Videoconferencing is defined as an interactive communication between two or more parties that utilize audio and video transmissions. Videoconferences provide a way for parties to meet without traveling great distances. It is different than broadcasting since each party has the ability to send as well as receive the audio and video signals. Videoconferences can use special equipment or simple peripherals added to a computer. The signals can travel through a number of different types of networks as long as all parties have access to the common communication path (Internet, ISDN lines, etc).

The International Telecommunications Union (ITU), Joint Picture Engineering Group (JPEG), and Motion Picture Engineering Group (MPEG) have released standards that are fundamental to video services interworking, as follows:

- The standard H.320 supports videoconferencing transmission using ISDN, as well as the sub standards H.323 (video communications over IP) and H.324 (videoconferencing over plain old telephone service [POTS]).
- In terms of video compression, the broadcast and video community agreed on JPEG, MPEG-2, and MPEG-4 as standards that provide compression guidelines to provide real-time broadcast video quality at 30 fps.
- The T.120 standard provides for the interoperability between the different document conferencing systems.

*Required Standards:*

- H.320 – Standard for addressing ISDN Videoconferencing <http://www.imtc.org/h320.htm>
- H.323 – Standard for addressing Video (Audiovisual) communication on Local Area Network. <http://www.imtc.org/h323.htm>

- H.324 – Standard for addressing High Quality Video and Audio Compression over POTS modem connections. <http://www.imtc.org/h324.htm>

**Table 4.12-1: Videoconferencing Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Microsoft</a>	NetMeeting	IP based Videoconferencing	Windows 2000	Local
<a href="#">Polycom</a>	Video Conferencing	ISDN based Videoconferencing	Video Conferencing	Local

**Table 4.12-2: Videoconferencing Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

### 4.13 Virtual LAN

With Virtual Local Area Network (VLAN) capability, network administrators can group geographically dispersed users in network-wide virtual topologies. A VLAN also provides easier management of network broadcast activity across the enterprise network.

A VLAN offers a fundamental change to how LANs are designed, administered, and managed. With VLAN switching technology, network managers can create networks based on logical groups independent of physical location. Users can be assigned to a workgroup no matter where they are physically located or to what LAN segment they are connected. A VLAN allows the ability to create, group, and regroup LAN segments logically and instantaneously, without changing physical infrastructure or taking down users and servers.

A VLAN can be viewed as a broadcast domain with logically configured boundaries. With the implementation of VLAN, all broadcasts are confined to a specific broadcast domain. VLAN broadcast domains are independent of physical location, the LAN media, the Media Access Control (MAC) type, and the transmission rates. Members can be located where they need to be rather than being forced to move to a specific location to connect to the LAN. Different members can also be on different physical media (Ethernet, Fiber Distributed Data Interface [FDDI], etc.) running at varied transmission rates. For example, all finance packets stay within Finance and are not transmitted to Marketing, Engineering, Sales, etc.

A VLAN offers the added benefit of security. Users in a defined group are prevented from eavesdropping on other groups because each VLAN is a closed, logically defined group. A VLAN provides substantial benefits in LAN administration such as improved security and management of network broadcast activity across the enterprise. VLANs are limited to the confines of a building with the exception of a management VLAN.

*Required Standard:*

- IEEE 802.1Q

**Table 4.13-1: VLAN Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Not used		Data Communications		

**Table 4.13-2: VLAN Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data Communications		

#### 4.14 Voice Over IP (VoIP)

Voice over IP (VoIP) is voice transmission over a data network. Standard voice communications require a separate network with resources dedicated between the two end points for the duration on the call. VoIP tries to take advantage of the efficiencies of IP-based data networks. The advantages include having one set of wires for both data and voice, and lowering the number of skills needed to support all of the networks.

Unfortunately, voice has additional requirements that standard IP networks are not designed to handle. Data, unlike voice, is not as time sensitive for transmission. Most IP networks make best effort in delivering packets with only first come, first serve as a priority model. Support for voice requirements are beginning to show up in newer IP network equipment. Another concern is the issue of combining the two networks. With two networks, if one goes down, then the other can be used to continue communications. Having only one network could halt communications completely if it failed.

*Required Standards:*

- H 225 - Call signaling protocols and media stream packetization for packet-based multimedia communication systems.  
<http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-H.225.0>
- H.323 v2/v3 ITU Standards, <http://www.imtc.org/h323.htm>

**Table 4.14-1: VoIP Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.14-2: VoIP Preferred Product for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

## 4.15 Communication Protocols

Data network interoperability addresses the need to deliver end-to-end services across physically and logically diverse data networks. Physically diverse networks include WANs, Internets, and Extranets. Logically diverse networks are defined by different hardware and software products used in their construction. If two systems are to communicate successfully they must use a common set of rules that both understand. A communications protocol is such a “set of rules” that defines, for example, a set of standard requests and responses, and the order in which they can be sent.

For an overview of Internetworking Technology, refer to [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/index.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm)

The following communication protocols are discussed in the next subsections:

- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Ethernet
- Wireless Local Area Network (WLAN)
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- Dynamic Host Configuration Protocol (DHCP)
- Hypertext Transfer Protocol (HTTP)
- Uniform Resource Locator (URL)
- Multipurpose Internet Mail Extensions (MIME)

### 4.15.1 Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)

Internetwork Packet Exchange (IPX) was developed by Novell as a network layer protocol responsible for addressing and routing packets to nodes on one or multiple subnets. Like TCP/IP, IPX works with network layer addresses, as opposed to physical layer addresses, which are assigned to the Network Interface Card (NIC) manufacturers.

IPX is a datagram service protocol that allows individual packets to be sent to and received from user processes. IPX is a connectionless service. It does not support the concept of a connection or reliable delivery. However, guaranteed services like Sequence Packet Exchange (SPX) have been built on top of IPX, hence IPX/SPX. IPX is used in situations where a guaranteed service is not required or where an occasional lost packet is not critical.

NetWare’s transport layer SPX protocol provides a connection-oriented link between nodes. The SPX protocol ensures that packets arrive at their destination with enough sequence information to reconstruct the message at the receiving end, and also to maintain a connection at a specified level of quality. To accomplish this, SPX is responsible for flow control, packet acknowledgment, and similar activities.

Network Basic Input/Output System (NetBIOS) is a LAN protocol for personal computers. Novell's NetBIOS emulator provides NetBIOS flows over its IPX protocol.

**Table 4.15-1: IPX/SPX Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Novell</a>	NetWare	IPX/SPX	x86-based Novell NetWare server	Local

**Table 4.15-2: IPX/SPX Preferred Products for Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		IPX/SPX to be phased out		

#### 4.15.2 Transmission Control Protocol / Internet Protocol (TCP/IP)

The Internet protocols consist of a suite of communication protocols, of which the two best known are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The Internet protocol suite not only includes lower-layer protocols (such as TCP and IP), but it also specifies common application level protocols for services such as electronic mail, terminal emulation, and file transfer.

The IP is a network layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP is documented in RFC 791 and is the primary network layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork; and providing fragmentation and reassembly of datagrams to support data links with different Maximum-Transmission Unit (MTU) sizes. IP is documented in RFC 793.

The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing. With stream data transfer, TCP delivers an unstructured stream of bytes identified by sequence numbers. This service benefits applications because they do not have to chop data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery.

TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. Bytes not acknowledged within a specified time period are retransmitted. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission.

TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence number it can receive without

overflowing its internal buffers. Full-duplex operation means that TCP processes can both send and receive at the same time.

The User Datagram Protocol (UDP) is a connectionless transport layer protocol (Layer 4) that belongs to the Internet protocol family. UDP is basically an interface between IP and upper-layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another. Unlike the TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP. Because of UDP's simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP. UDP is useful in situations where the reliability mechanisms of TCP are not necessary, such as in cases where a higher-layer protocol might provide error and flow control. UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Trivial File Transfer Protocol (TFTP).

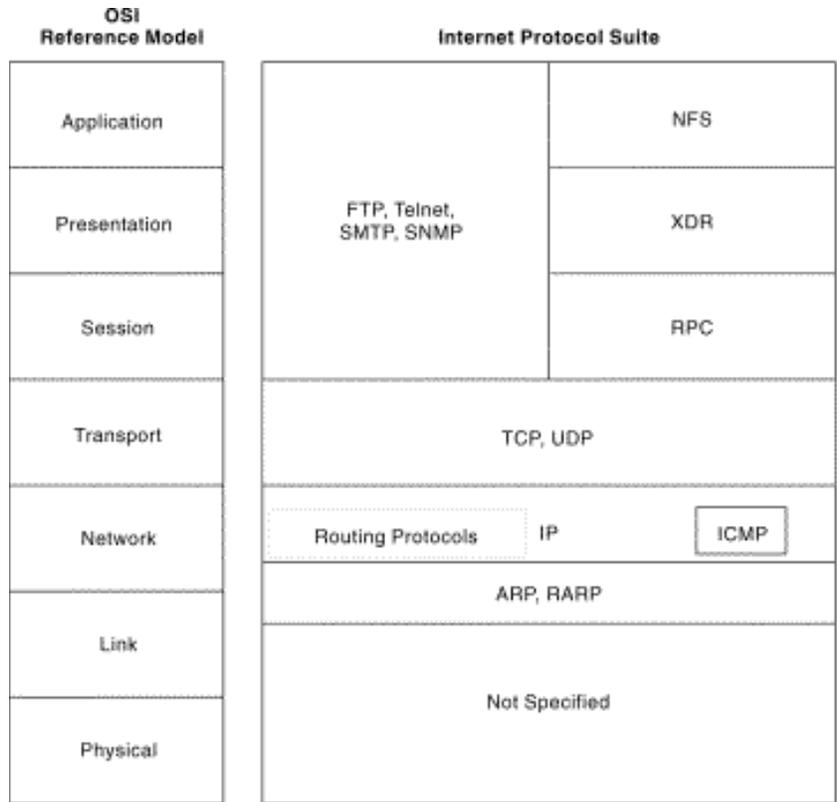
The TCP/IP protocol suites also include Application Layer Protocols:

- File Transfer Protocol (FTP) – Moves files between devices.
- Simple Network-Management Protocol (SNMP) – Primarily reports anomalous network conditions and sets network threshold values.
- Telnet – Serves as a terminal emulation protocol.
- X Windows – Serves as a distributed windowing and graphics system used for communication between X terminals and UNIX workstations.
- Network File System (NFS), External Data Representation (XDR), and Remote Procedure Call (RPC) – Work together to enable transparent access to remote network resources.
- Simple Mail Transfer Protocol (SMTP) – Provides electronic mail services. SMTP is the TCP/IP standard protocol that provides the exchange of mail between network computers and specifies the exact format of the message to be sent from an SMTP client operating on one computer system to and from an SMTP server on another.  
<http://www.faqs.org/rfcs/rfc-index.html>.
- Domain Name System (DNS) – Translates the names of network nodes into network addresses.

For further information, refer to:

- [http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/ip.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip.htm) and <http://www.protocols.com/pbook/tcpip.htm>.

OSI Reference Model: The 1984 release of the OSI (“7 Layer”) model by the International Standards Organization (ISO) has become an international standard and serves as a guide for networking. The OSI model is an architecture that divides network communication into seven layers. Each layer covers different network activities, equipment or protocols, as shown in the figure below.



**Figure 4.15-1: Mapping of the TCP/IP Suite to the OSI Model**

*Required Standards:*

- RFC791 (IP)
- RFC793 (TCP)
- RFC768 (UDP)
- RFC 821 (SMTP)

For further information on RFCs, refer to:

<http://www.rfc-editor.org/rfcxx00.html#STDbyRFC> and search by RFC#.

**Table 4.15-3: TCP/IP Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
OS Vendor	TCP/IP	TCP/IP as the default communication protocol	All	ALL

**Table 4.15-4: TCP/IP Preferred Products for the Judiciary**

<b>Vendor</b>	<b>Product</b>	<b>Function</b>	<b>Judiciary Platform</b>	<b>Scope</b>
OS Vendor	TCP/IP	Default communication protocol	All	ALL

#### **4.15.2.1 Internet Control Message Protocol (ICMP)**

The Internet Control Message Protocol (ICMP) is a network layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source.

ICMPs generate several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement and Router Solicitation. If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages.

When an ICMP destination-unreachable message is sent by a router, it means that the router is unable to send the package to its final destination. The router then discards the original packet. A destination might be unreachable because the source host has specified a nonexistent address. Less frequently, the router does not have a route to the destination.

*Required Standards:*

- RFC 792 (ICMP)

#### **4.15.2.2 Address Resolution Protocol (ARP)**

For two machines on a given network to communicate, they must know the other machine's physical or Media Access Control (MAC) addresses. By broadcasting Address Resolution Protocols (ARPs), a host can dynamically discover the MAC-layer address corresponding to a particular IP network layer address.

After receiving a MAC-layer address, IP devices create an ARP cache to store the recently acquired IP-to-MAC address mapping, thus avoiding having to broadcast ARPs when they want to reconnect a device. If the device does not respond within a specified time frame, the cache entry is flushed.

#### **4.15.2.3 Routing Protocols**

Routing protocols are protocols that implement routing algorithms. Put simply, routing protocols direct protocols through an internetwork. Examples of these protocols include Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP), Open Shortest Path First (OSPF), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), and Routing Information Protocol (RIP).

Currently, the Judiciary uses Enhanced IGRP as the routing protocol. Products used to support these protocols are listed in Chapter 5 under Communications Hardware. At the perimeter network, the Judiciary uses Border Gateway Protocol (BGP).

### 4.15.3 Ethernet

Ethernet is a LAN technology that transmits information between computers at speeds of 10 and 100 million bits per second (megabits - Mbps), and 1 billion bits per second (gigabits - Gbps) as specified in standard, IEEE 802.3. An Ethernet LAN now typically uses special grades of Unshielded Twisted Pair (UTP) wires. Devices connected using Ethernet technology, including the original 10 Mbps system, 100 Mbps Fast Ethernet, and Gigabit Ethernet, compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.

10 Mbps Ethernet (IEEE 802.3) provides transmission speeds up to 10 Mbps. There are four baseband media segments defined in the 10-Mbps Ethernet standard: 10BASE5, 10BASE2, 10BASE-T, and 10BASE-F. These four media types are shown with their IEEE shorthand identifiers. The IEEE identifiers include three pieces of information. The first item, 10, stands for the media speed of 10-Mbps. The word BASE stands for baseband, which is a type of signaling. Baseband signaling simply means that Ethernet signals are the only signals carried over the media system. The third part of the identifier provides a rough indication of segment type of length. For thick coaxial cable (i.e., thicknet), the 5 indicates the 500-meter maximum length allowed for individual segments of cable. For thin coaxial cable (i.e., thinnet) the 2 is rounded up from the 185-meter maximum length for individual cable segments. The T and F stand for twisted-pair and fiber optic, respectively, and indicate the cable type. The thick coaxial media segment was the first defined in the earliest Ethernet specifications. This was followed by the thin coaxial segment, and then the twisted-pair and fiber optic media segments.

Fast Ethernet (IEEE 802.3u) is also known as 100BASE-T. This LAN standard raised the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. The Fast Ethernet specification calls for three types of transmission schemes over various wire media: 100BASE-TX, 100BASE-FX, and 100BASE-T4. 100BASE-TX uses Category 5, unshielded, twisted-pair copper cable to connect the various hubs, switches, and end-nodes together. 100BASE-FX uses 62.5/125 multimode fiber-optic cable to transport Fast Ethernet traffic. 100BASE-T4 incorporated the use of two more pairs of wiring to allow Fast Ethernet to operate over Category 3-rated cables or above.

For further information on Ethernet, refer to <http://www.ots.utexas.edu/ethernet/ethernet-home.html>.

#### *Required Standards:*

- IEEE 802.3 (ISO 8802)
- The IEEE 802.3, 2000 Edition (also ISO/IEC 8802-3:2000) are available at: <http://standards.ieee.org/catalog/IEEE802.3.html> or refer to [http://www.iso.ch/iso/en/Standards\\_Search.StandardsQueryForm](http://www.iso.ch/iso/en/Standards_Search.StandardsQueryForm) and search for ISO # 8802.
- IEEE 802.3u
- IEEE 802.3z

**Table 4.15-5: Ethernet Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
	IEEE 802.3	LAN protocol	All	ALL

**Table 4.15-6: Ethernet Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
	IEEE802.3z	LAN protocol	All	ALL

### 4.15.3.1 Gigabit Ethernet

Gigabit Ethernet provides a higher level of backbone support at 1000 Mbps (gbps or 1 billion bits per second). There are two standards, IEEE 802.3z or 1000BASE-X and IEEE 802.3ab or 1000BASE-T. IEEE 802.3z is the standard for fiber-based Gigabit Ethernet and IEEE 802.3ab is for copper-based Gigabit Ethernet.

Gigabit Ethernet distance specifications for fiber optic media vary depending on the type of fiber and transceiver used. For the 62.5 micron diameter 160 MHz\*km multimode (MM) fiber, often called FDDI-grade fiber, the distance is specified at 220 meters. As the bandwidth of the fiber increases, the maximum range for MM fiber increases up to 550 meters. The long-wave length transceiver (1000BASE-LX) reaches 550 meters for all media types. For single mode fiber with 1000BASE-LX, the distance is specified at 5 kilometers.

Two physical layers (PHYs) provide Gigabit transmission over fiber-optic cabling. 1000BASE-SX is targeted at lowest-cost multimode fiber runs in horizontal and shorter backbone applications. 1000BASE-LX is targeted at longer multimode building fiber backbones and single-mode campus backbones. For multimode fiber, these standards define gigabit transmission over maximum distances ranging from 220 to 550 meters. Single-mode fiber, which is covered by the long-wavelength standard, is defined to cover distances of 5 kilometers.

There is also a standard IEEE 802.3ab or 1000BASE-T for Gigabit Ethernet transmission over copper cabling. 1000BASE-T is one of the four physical layers or transceivers defined by the two Gigabit Ethernet standards: IEEE 802.3z or 1000BASE-X and IEEE 802.3ab or 1000BASE-T. 1000BASE-X supports multimode and single-mode fiber media and a short-reach, 25-meter copper jumper. Because most of the cabling installed inside buildings today is Category 5 copper UTP, the IEEE 802.3 1000BASE-T standard was designed to support Gigabit Ethernet operation over the Category 5 cabling systems installed according to the specifications of ANSI/TIA/EIA-568A (1995).

1000BASE-T works by using all four of the Category 5 pairs to achieve 1000 Mbps operation over the installed Category 5 copper cabling. 1000 Mbps data rates are achieved by sending and receiving a 250 Mbps data stream over each of the four pairs simultaneously (4 X 250 Mbps = 1 Gbps). 1000BASE-T will run on Category 5 and Category 5e cabling at distances to 100 meters.

In contrast, 100BASE-TX uses two pairs: one to transmit and one to receive. Fast Ethernet on copper (100BASE-TX) achieves 100 Mbps operation by sending encoded symbols across the

link at a symbol rate of 125 Mbaud. A 125 Mbaud symbol rate is required because the 100BASE-TX encoding scheme (called 4B/5B coding) has a bandwidth overhead of 20 percent, the difference between 100 Mbps and 125 Mbaud. Although 1000BASE-T uses a different encoding scheme (five level pulse amplitude modulation or PAM-5), because it maintains the 125 Mbaud symbol rate of 100BASE-TX, 1000BASE-T is backwards compatible with 100BASE-FX at the physical layer.

*Required Standards:*

- IEEE 802.3z or IEEE 802.3ab.  
<http://standards.ieee.org/catalog/IEEE802.3.html>,  
<http://www.gigabit-ethernet.org>, or <http://www.10gea.org/Tech-whitepapers.htm> for latest information

**Table 4.15-7: Gigabit Ethernet Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
	IEEE 802.3	LAN protocol	All	ALL

**Table 4.15-8: Gigabit Ethernet Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
	IEEE 802.3z	LAN protocol	All	ALL

#### 4.15.4 Wireless Local Area Network

Wireless Local Area Network (WLAN) provides the features and benefits of LAN technologies without wires or cables. Instead of twisted-pair or fiber-optic cable, WLANs use either Infrared Light (IR) or Radio Frequency (RF) as the transition medium. Most of the wireless LANs use RF technology and the 2.4GHz frequency band, and allow workstations or other devices to communicate in a network.

Wireless networking uses multiple frequencies to break up the data transmission and reduce the occurrence of blocked or corrupted transmissions. The radio spectrum used for wireless networking includes 900 Mhz and 2.4 Ghz, which is also used for cordless telephones. Wireless network protocols use collision-sensing and correcting-transmission mechanisms Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) analogous to the Ethernet Carrier Sense Multiple Access/Collision Detection (CSMA/CD).

The **DECT** (Digital European Cordless Telephone) chipset family is a highly integrated solution for 1.9GHz cordless telephones for the **DECT** 1.9GHz Band. The **DECT** chipset provides a 3-chip solution: the Baseband controller (DE56xxx), the RF Transceiver (DE19RF16), and a simple external RF Power Amplifier (DE19PA16) required to boost the output power to the maximum allowed level.

Link: <http://www.dspg.com/dspg/dect.html>

Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) protocols are used to complete the “handshaking” initial contact between wireless network nodes, such that frequency switching is synchronized. Under DSSS the transmitter switches frequencies in a preordained sequence; data is divided into chips (packets), which are sent at different frequencies and reassembled by the receiving station. FHSS also uses a series of transmission frequencies. Data is transmitted during dwell time while the transmitter and receiver are on the same discrete frequency.

#### 4.15.4.1 IEEE 802.11 Specifications

802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

There are several specifications in the 802.11 family:

- **802.11** -- applies to wireless [LANs](#) and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either [frequency hopping spread spectrum](#) (FHSS) or [direct sequence spread spectrum](#) (DSSS).
- **802.11a** -- an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an [orthogonal frequency division multiplexing](#) encoding scheme rather than FHSS or DSSS.
- **802.11b** (also referred to as *802.11 High Rate* or [Wi-Fi](#)) -- an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- **802.11g** -- applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.

The 802.11b WLAN standard was released by IEEE in June 1997 and provides a full Ethernet-like data rate of 11Mbps over DSSS transmission method. Spread spectrum is a modulation technique developed in the 1940s that spreads a transmission signal over a broad band of radio frequencies. It is less susceptible to radio noise and creates little interference.

The WLAN requires Access Point products and wireless network cards for PCs or laptops and other devices to access the network. An access point serves several functions in a WLAN. In many networks, it is used to connect the wireless portion of a network to a hardwired Ethernet network. An access point also can act as a repeater. It can receive a signal from one wireless node and transmit it to another.

*Required Standards:*

- IEEE 802.11b
- IEEE 802.11a
- IEEE 802.11g

Refer to [http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/airo\\_ov.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/airo_ov.htm) for further information.

**Table 4.15-9 WLAN Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.15-10: Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Wireless LAN	Wireless LAN	ALL

#### 4.15.5 Frame Relay

Frame relay is a Wide Area Network (WAN) technology based on a packet-oriented communication technology. Frame relay service is primarily used for LAN interconnections over public or private networks. It also used for voice and video transmission under certain circumstances. Frame relay is a fast-packet technology that requires a dedicated connection during the transmission period. In data communication, a fast packet transmits data among networks without any error checking at points along the route. It is assumed that the underlying network is reliable and that any errors (such as lost or corrupt packets) will be handled by higher-layer protocols such as IP. The assurance that the packet arrived without error is the responsibility of the end points or the receiver. Frame relay relays packets at the data-link layer of the OSI model rather than at the network layer. A frame relay connection is known as a virtual connection. A permanent virtual connection is totally dedicated to one origin and destination pair and can transmit up to 1.544 Mbps, depending on the capabilities of the pair. A switched virtual connection is also possible using the public network and can provide higher bandwidths.

For an overview of frame relay see:

[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/frame.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/frame.htm).

**Table 4.15-11: Frame Relay Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Sprint	FTS2001	Data Communications	DCN WAN	ALL

**Table 4.15-12: Frame Relay Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Sprint	FTS2001	Data Communications	DCN WAN	ALL

#### 4.15.6 Asynchronous Transfer Mode

Asynchronous Transfer Mode (ATM) is a high-speed, physical-layer transfer mode which supports voice, video, and data using fixed-length cells. ATM also supports constant bit rate and sporadic high-volume transmissions. ATM is a versatile and multifunctional platform that can support a variety of services and traffic types. It uses a switch-based technology that may be

applied to LAN and WAN environments that can accommodate bandwidth requirements for complex networked applications.

The layered ATM architecture is what allows multiple services like voice, data, and video to be mixed over a network. Using ATM, information to be sent is segmented into fixed-length cells, transported to, and re-assembled at the destination. ATM is a hardware-implemented packet switching protocol that has a fixed cell length of 53 bytes. A fixed length allows the information to be transported in a predictable manner. This predictability accommodates different traffic types on the same network.

The ATM cell is broken into two main sections, the header and the payload. The header is 5 bytes long and is used for routing the information through the network. ATM switches use routing tables to determine a destination port for the cell at each switch. The payload (48 bytes) is the portion that carries the actual information, either voice, data, or video.

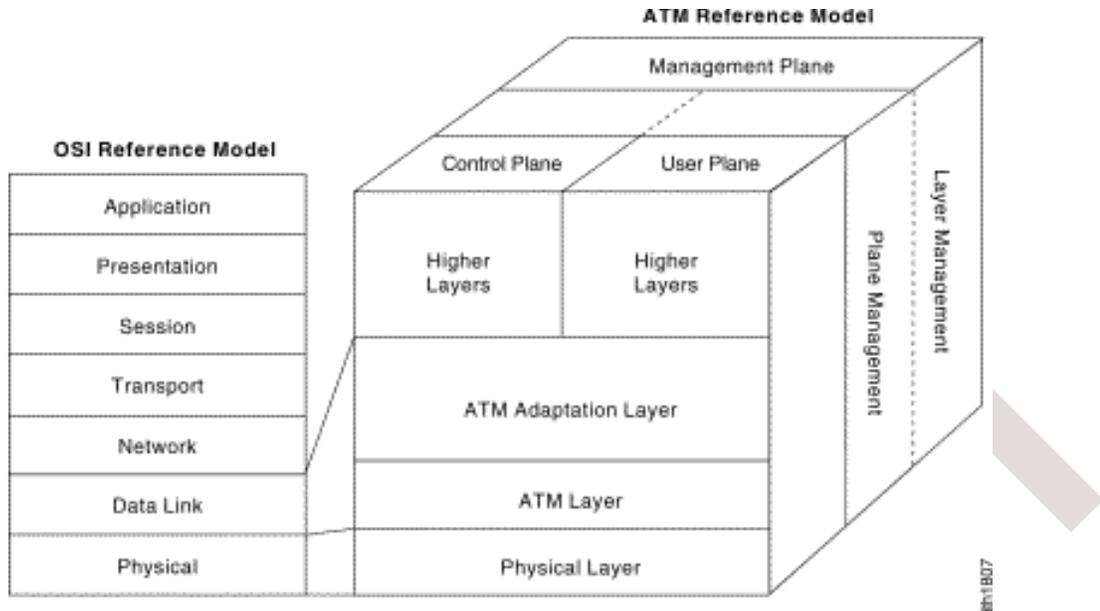
For further information, refer to:

[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/atm.htm#xtocid129392](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/atm.htm#xtocid129392).

ATM is based on the efforts of the ITU-T Broadband Integrated Services Digital Network (BISDN) standard. It was originally conceived as a high-speed transfer technology for voice, video, and data over public networks. The ATM Forum extended the ITU-T's vision of ATM for use over public and private networks. The ATM Forum has released work on the following specifications:

- User-to-Network Interface (UNI) 2.0
- UNI 3.0
- UNI 3.1
- Public-Network Node Interface (P-NNI)
- LAN Emulation (LANE)

Figure 4-15.2 shows that the ATM reference model relates to the lowest two layers of the OSI reference model.



**Figure 4.15-2: ATM Reference Model**

*Required Standards:*

- Open System Interconnection (OSI)
- Specifications and standards are those adopted by the ATM Forum and the Internet Engineering Task Force (IETF)
- Standard for Multi-Protocol over ATM (MPOA) is deployed on the network
- Standard for Multi-Protocol over ATM version 1.1 <ftp://ftp.atmforum.com/pub/approved-specs/af-mpoa-0114.000.pdf>
- Standard for silence suppression, voice compression, and variable-bit-rate (VBR) service will emerge

**Table 4.15-13: ATM Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Not used		Data Communications		

**Table 4.15-14: ATM Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data Communications		

#### 4.15.6.1 LAN Emulation

To support existing applications operating in a LAN with Ethernet, an ATM network must have an interface at the desktop, end stations, and router to emulate the behavior of a shared media LAN, such as Ethernet. LAN Emulation (LANE) provides such an interface. ATM LAN emulation allows a connection-oriented network to function as a connectionless LAN. The software is directly above the AAL5 and directly below the MAC sub-layer of the data link layer.

*Required Standards:*

- The ATM Forum’s LANE version 1.0  
<ftp://ftp.atmforum.com/pub/approved-specs/af-lane-0021.000.pdf>
- IEEE 802.3 Ethernet

**Table 4.15-15: LANE Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Not used		Data Communications		

**Table 4.15-16: LANE Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data Communications		

#### 4.15.6.2 Emulated LAN

In environments where there is a need to configure multiple, separate domains within a single network, the definition of an Emulated LAN (ELAN) comprising a group of ATM-attached devices is required. Several ELANs may be configured within an ATM network, and membership in an emulated LAN is independent of where an end system is physically connected. An end system could belong to multiple ELANs. Each ELAN consists of a LAN Emulation Configuration Server (LECS), LAN Emulation Server (LES), Broadcast and Unknown Server (BUS), and LAN Emulation Clients (LEC).

**Table 4.15-17: ELAN Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Not used		Data Communications		

**Table 4.15-18: ELAN Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data Communications		

### 4.15.6.3 Multi-Protocol Over ATM

Multi-Protocol Over ATM (MPOA) integrates OSI layer 3 protocols with the ATM layer. The ATM LANE) described in Section 4.15.6.1 is designed to allow inter-working between legacy LAN networks and ATM. MPOA adds to LANE the integration of Layer 3 protocols with the ATM layer. MPOA allows the ATM layer to be used to provide direct communication between ATM edge devices and hosts regardless of the logical Layer 2 or Layer 3 topology on the network. A network using MPOA benefits from the control and broadcast isolation provided by Layer 3 routing without the delay and throughput bottlenecks of routers. This is accomplished by separating the transport of data and control information. Data flow on shortcut Virtual Channel Connections (VCC) which follows the optimal path through the ATM network while Layer 2 and Layer 3 routing protocols follow the logical topology of ELANs and routers over-laid on the ATM network. MPOA specifies two logical components that combine to form a virtual router.

*Required Standards:*

- Open System Interconnection (OSI)
- Multi-Protocol Over ATM Version 1.1
- <ftp://ftp.atmforum.com/pub/approved-specs/af-mpoa-0114.000.pdf>

**Table 4.15-19: MPOA Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Not used		Data Communications		

**Table 4.15-20: MPOA Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data Communications		

### 4.15.7 Dynamic Host Configuration Protocol

Tracking network IP addresses can become difficult if there is no automated device to manage such work. It may require tracking additions and moving among thousands of remote and local users distributed in various subnets stretched across the Judiciary enterprise network. Duplicate IP addresses can result, causing devices with the same IP address to lock up. This problem becomes heightened when connected to the Internet, Intranet or Extranet, as each IP address has to be unique among the many devices registered.

The Dynamic Host Configuration Protocol (DHCP) provides a framework for managing client and server IP configurations. It supports the automatic allocation of IP addresses and configuration parameters to clients. DHCP programs automatically assign or lease an IP address to a device when it connects to the network. The device, such as a network PC, issues a request at startup; the server receives the request and issues the client an IP address. The address issued to the device could be a permanent address, generally called a static address, or a temporary address for a specified time, usually called a leased address.

DHCP servers can be used to automatically and dynamically assign TCP/IP configuration parameters such as an IP address, subnet mask, and the default gateways to clients on Network Operating Systems.

DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a client; and a mechanism for the allocation of network addresses to clients.

DHCP servers can support three methods of address assignment: manual, automatic, and dynamic. A particular network will use one or more of these mechanisms, depending on the policies of the network administrator.

In manual allocation, a host's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the host, based on the MAC address of the PC's network interface card.

In automatic allocation, the DHCP server allocates addresses from a pool of available addresses that are specified by the network administrator. Once allocated, the IP address is permanent until manual intervention.

In dynamic allocation, the DHCP server allocates addresses from a pool of addresses for a specified length of time, called the lease period. At the end of this period, if a client has not renewed a lease, its IP address is returned to the server's pool.

*Required Standards:*

- RFC 2131, Dynamic Host Configuration Protocol—an Internet Proposed Standard Protocol by Dynamic Host Configuration Working Group of the Internet Engineering Task Force (IETF)

**Table 4.15-21: DHCP Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
	LAN switches and routers	DHCP Server	LAN	Local
OS Vendor	DHCP	DHCP Server	x86-based server	Local

**Table 4.15-22: DHCP Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
	LAN switches and routers	DHCP Server	LAN	Local
OS Vendor	DHCP	DHCP Server	x86-based server	Local

#### 4.15.8 Hypertext Transfer Protocol

The Hypertext Transfer Protocol (HTTP) is the basic protocol for the World Wide Web. It is an application-level protocol for distributed, collaborative, hypermedia information systems. Data transferred by the protocol can be plain text, hypertext, audio, images, or any Internet-accessible information. HTTP works when users click on a hyperlink with URLs that begin with `http://`. Once activated, HTTP features a four-part process that consists of the following stages: connection, request, response, and disconnect (or close). The request is sent by a client, such as a web browser, to the server; a response is then returned by the server. The server is where a resource resides, such as a web server where a desired home page is located.

The HTTP client sends a request to the server in the form of a request method, Uniform Resource Identifiers (URIs), and protocol version, followed by a MIME<sup>1</sup>-like message containing request modifiers, client information, and possible body content. The server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity body content.

The TCP connection between the client and the server is an end-to-end operation. There are one or more intermediary systems with TCP connections between logically adjacent systems. Each intermediary system acts as a relay, so that a request initiated by the client is relayed through the intermediary systems to the server, and the response from the server is relayed back to the client. The HTTP specification defines three forms of intermediary systems: proxy, gateway, and tunnel. HTTP is used as a generic protocol for communication between clients and proxies/gateway to other Internet systems, including those supported by SMTP, FTP, Gopher, and Wide Area Information Server (WAIS) protocols. In this way, HTTP allows basic hypermedia access to resources available from diverse applications.

A proxy is an intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly with translation, to other servers. A proxy **MUST** implement both the client and server requirements of this specification. A transparent proxy is a proxy that does not modify the request or response beyond what is required for proxy authentication and identification. A non-transparent proxy is a proxy that modifies the request or response in order to provide added service to the user agent, such as group annotation services, media type transformation, protocol reduction, or anonymity filtering. Except where either transparent or non-transparent behavior is explicitly stated, the HTTP proxy requirements apply to both types of proxies.

A gateway is a server, which acts as an intermediary for another server. Unlike a proxy, a gateway receives requests as if it were the origin server for the requested resource; the requesting client may not be aware that it is communicating with a gateway.

A tunnel is an intermediary program that acts as a blind relay between two TCP connections. Once active, a tunnel is not considered a party to the HTTP communication, even though the

---

<sup>1</sup> Multipurpose Internet Mail Extensions (MIME) is described in Communications Protocols, Section 4.15.10. The relationship between HTTP and MIME is described in appendix 19.4 of the Hypertext Transfer Protocol -- HTTP/1.1, Network Working Group, W3C/MIT June 1999, <ftp://ftp.isi.edu/in-notes/rfc2616.txt>.

tunnel may have been initiated by an HTTP request. The tunnel ceases to exist when both ends of the relayed connections are closed.

*Required Standards:*

- RFC 2774, Hypertext Transfer Protocol HTTP/1.1, February 2000, by the Internet Engineering Task Force/W3C (IETF/W3C) HTTP development group  
<http://www.w3.org/Protocols>.

#### 4.15.9 Uniform Resource Locator

A Uniform Resource Locator (URL) provides a standard written pathway to specify the location of a resource on the Internet. When a user requests resources from the Internet and types a URL into the browser, the URL is mapped to an IP address and port corresponding to a specific web server. The URL allows users to browse the Web, jump to a specific site, or make a connection to a target Web site.

The URL has three basic sections: protocol, server name, and file identification. URLs specify the access method or protocol (how), the server name (where), and the file identification (what) needed for a Web client to find and access an object. The general form of a URL is:

Access method or protocol://server name [:port]/file identification

The access method or protocol portion of the URL is the way the browser communicates with the server. It determines which protocol the browser uses to contact the server. In most cases, the standard protocol is either http, ftp, gopher, or WAIS. There are two instances in which the protocol type might be omitted from a URL. The protocol is left off when using a browser that can detect the protocol type from the remote server. The protocol is also unnecessary when referring to a file located on the same server as the referring link. In these cases, the URL is referred to as a partial URL. In the protocol portion of a URL, the protocol is followed by a colon and two forward slashes, as in <http://aoweb>.

The server name portion of the URL is an IP host name or an IP address. It identifies the server where the information resides. Most servers use default port numbers so the port number is usually not needed.

The file identification portion of the URL identifies the location, or path and name, of the file requested; it can include the directory, subdirectory, or file name.

For example, the URL to register with the PACER service center is:

<http://pacер.psc.uscourts.gov/register.html>

where:

**http** is the access method or protocol

**pacер.psc.uscourts.gov** is the server name or Intranet address of the server

**/register.html** is the file identification/path of the file

*Required Standards:*

- RFC 2700, August 2000 - Internet Engineering Task Force (IETF) Network Working Group  
<http://www.ietf.org/rfc/rfc2700.txt?number=2700>

#### 4.15.10 Multipurpose Internet Mail Extensions

Multipurpose Internet Mail Extensions (MIME) extends the format of Internet mail to allow non-US-ASCII textual messages, non-textual messages, multipart message bodies, and non-US-ASCII information in message headers.

*Required Standards:* The following Requests For Comments (RFCs) at the following link define MIME: <http://www.oac.uci.edu/indiv/ehood/MIME/MIME.html>

- RFC 2045: MIME Part One: Format of Internet Message Bodies
- RFC 2046: MIME Part Two: Media Types
- RFC 2047: MIME Part Three: Message Header Extensions for Non-ASCII Text
- RFC 2048: MIME Part Four: Registration Procedures
- RFC 2049: MIME Part Five: Conformance Criteria and Examples

Refer to <http://www.rfc-editor.org/rfc.html> or <http://www.rfc-editor.org/rfcxx00.html#STDbyRFC> for further information.

**Table 4.15-23: MIME Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Sun	Solaris (mail server)	Internet E-Mail gateway	Sun SPARC	AO <sup>1</sup>
<a href="#">IBM</a> / Lotus Development Corp.	Notes	E-Mail	Lotus Notes server	ALL

**Table 4.15-24: MIME Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Sun	Solaris (mail server)	Internet E-Mail gateway	Sun SPARC	AO <sup>1</sup>
<a href="#">IBM</a> /Lotus Development Corp.	Notes	E-Mail	Lotus Notes server	ALL

---

<sup>1</sup> AO (IMD)

## 4.16 Security Services

The technical aspects of security services may be handled by any combination of end applications, monitoring systems, message handling systems, network components, and operating systems. The actual selection of technologies used in implementing security should be based on interoperability, ease of implementation and administration, and general applicability across the enterprise. The major challenge in security is not the actual implementation methods, but the manner in which these methods are structured, administered, and how they interoperate with each other.

Security services include:

- Network Security Services
- Authentication
- Access Control
- Confidentiality, Data Integrity, and Non-repudiation
- Security Administration

### 4.16.1 Network Security Services

The Judiciary requires several types of connectivity between its internal network (DCN) and outside networks: Internet access, PacerNet access, other government networks, and remote access. Providing remote network access over public telephone lines allows anyone to dial a number and reach the door leading into a network. Internet access also allows everyone to reach the door. The Internet is a public network where millions of computers are connected together and is inherently insecure. As data is transmitted between the sender and receiver, it typically traverses through several other devices (e.g., routers), thereby allowing computers other than the sender and receiver to access the data. Even computers not directly involved in routing can access the data. These doors, therefore, are a potential means for would-be intruders to access internal Judiciary computer systems. The DCN itself is a WAN composed of line connecting sites across the United States.

In general, attacks on computer systems may be divided into three basic categories:

- **Intrusions**, where people can use the computer as if they were legitimate users.
- **Denial of service attacks**, aimed at preventing the legitimate users from using the computers. An intruder may flood a system or network with messages processes or network requests that prevent legitimate work from being done.
- **Information theft** usually exploits Internet services that are intended to give out information. Many Internet services are designed for use on LANs, and do not have the type or degree of security that allow them to be used safely across the Internet. For example, network taps, which are often called *sniffers*, are very effective at finding password information.

Because of the potential for attacks, the primary concern of Internet access and remote access security is to make sure that only known, authorized users can enter the door and that data can be securely transferred. Sending data across a network involves three other basic security risks:

- Eavesdropping – Intermediaries listen in on private conversations (one computer talking to another).
- Manipulation – Intermediaries change information in a private communication.
- Impersonation – A sender or receiver communicates under false identification.

Security measures, such as a firewall, authentication, and other privacy enhancement mechanisms are used to secure a network against intrusion, and to ensure that all communications between an internal network and the Internet are effectively protected. The design incorporates multiple levels of access and control, and is based on a layered protection and detection approach. It requires a security infrastructure that includes firewall servers and firewall rule sets, perimeter network(s) with multiple De-Militarized Zones (DMZs) that separate internal DCN traffic from the Internet and intrusion detection systems (IDSs).

#### **4.16.1.1 Secure Firewall**

Firewall technology provides client authentication for remote access, encryption for handling private communications over public networks, and address translation to help administrators deal with the overhead of limited Internet Protocol addresses. There are several industry standards used by firewall (and VPN) products, including the [Common Criteria for Information Technology Security Evaluation \(CC\) Version 2.1 / ISO IS 15408](#) and [Federal Information Processing Standard 140-1 \(FIPS 140-1\)](#). Another common industry certification is the International Computer Security Association ([ICSA](#)) ([www.icsa.net](http://www.icsa.net)), a membership organization founded in 1989 with the purpose of providing education and serving as a clearing house for computer security issues.

The Common Criteria is a mutually recognized international certification for security functionality assessment. There are seven evaluation assurance levels (EALs). EAL 2 is designated as structurally tested and EAL 4 is designated as methodologically designed, tested, and reviewed.

FIPS 140-2 is a standard that describes federal government requirements that IT products should meet for sensitive but unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST) and has also been adopted by the Canadian government's Communication Security Establishment (CSE). It defines the security requirements that must be satisfied by a cryptographic module used in a security system protecting unclassified information within IT systems. There are four levels of security ranging from Level 1 (lowest) to Level 4 (highest). These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be deployed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/electromagnetic

compatibility (EMI/EMC), and self-testing. For more information, please refer to <http://csrc.nist.gov/cryptval/>.

*Required Standards:*

- [Common Criteria for Information Technology Security Evaluation \(CC\) Version 2.1/ISO IS 15408](#)
- [FIPS 140-1](#)

**Table 4.16-1: Security Firewall Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	PIX	Firewall Security	Internet Gateway	ALL
Novell	Bordermanager	Firewall Security	N/A	ALL

**Table 4.16-2: Security Firewall Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	PIX	Firewall Security	Internet Gateway	ALL
Novell	Bordermanager	Firewall Security	N/A	ALL

#### 4.16.1.2 Intrusion Detection

The firewall server inspects each TCP/IP-based packet requiring access to and from the network(s) to which the firewall is connected. It examines network traffic based on a set of predefined rules that are uploaded from the firewall management station and can authenticate users with either a Judiciary authentication server, or a database stored on an LDAP server. It serves as a protective layer between the Judiciary's internal enterprise network and the outside networks.

Firewalls do a very good job of filtering incoming traffic from the Internet; however, as there are ways to circumvent them, they may not be sufficient to protect against attacks originating from the Internet. Firewalls are designed to allow authorized packets in and disallow others. An Intrusion Detection System (IDS) complements the firewall by detecting if those tunnels through the firewall are being exploited. Sometimes, firewalls and filtering techniques fail because of user configuration errors, hardware failure, or for a number of other causes. IDS can then function as a second line of defense. Some users may install new types of software with unknown or proprietary protocols that are not protected by the firewall. In many cases, such protocols are detected by an IDS.

An IDS monitors computer systems and network traffic and analyzes that data for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the enterprise. The main advantage of an IDS is that it provides a view of both network and server activity and issues alerts notifying administrators of unauthorized or unusual activity.

Currently two primary types of IDS are available: network-based and host-based. The two types are complementary. Network-based IDS are very good at providing an early warning of attacks. By monitoring the traffic stream in real-time, network sensors can see a threat and often neutralize it before it has a chance to do any damage. However, network sensors cannot advise whether an attack was successful or not. The information they gather is network-centric. Host-based IDS complement their network counterparts. Host-based sensors provide confirmation of an attack's success or failure and they yield system-specific event data, such as user name and file name during an unauthorized access attempt.

Figure 4-16.1 below depicts the Judiciary's national gateway IDS.

# Gateway & WAN Networks Security Domains

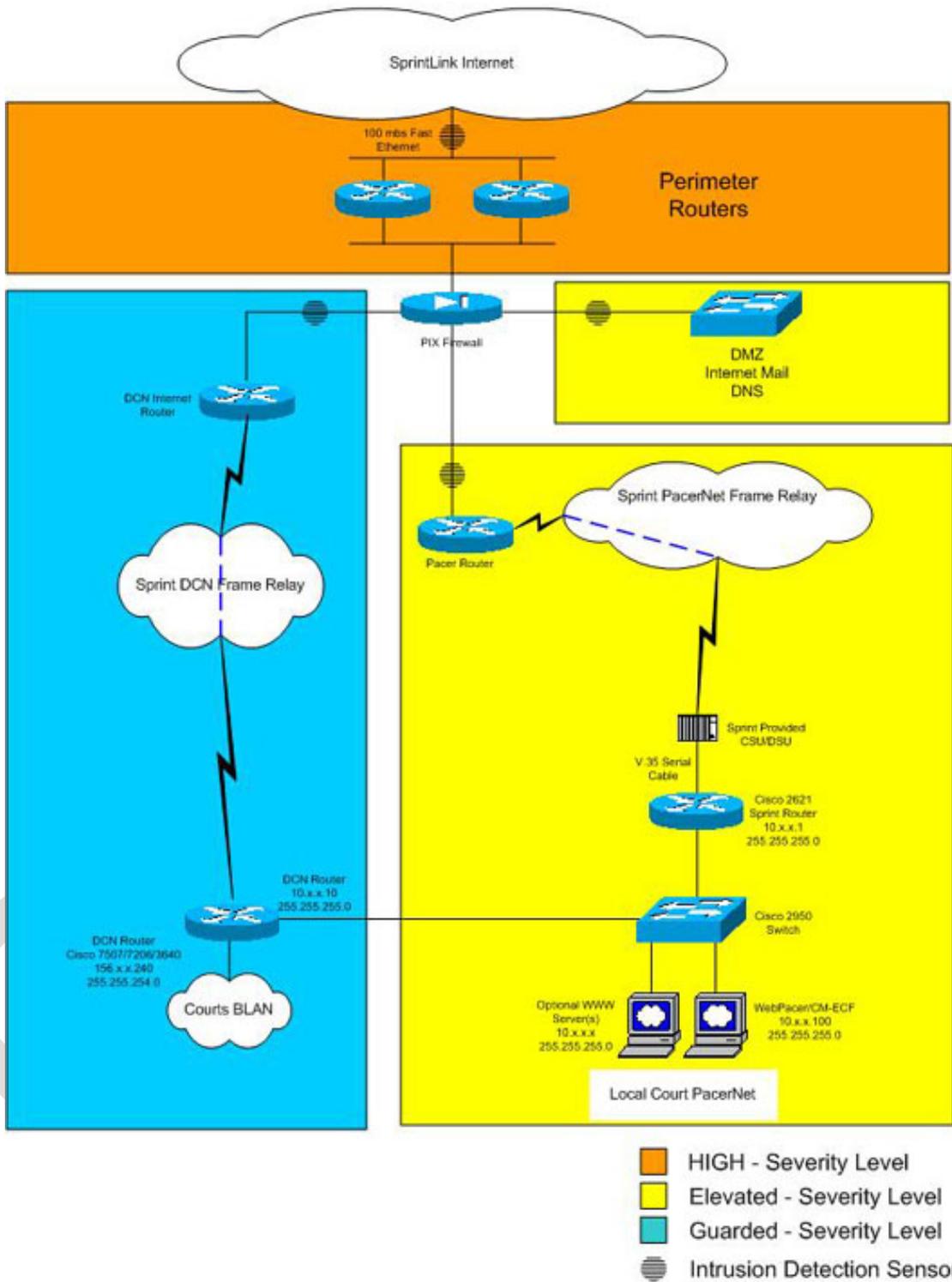


Figure 4.16-1: National Gateway Intrusion Detection System (IDS)

*Required Standard:*

There is an industry standard group, the Intrusion Detection Working Group (IDWG) that has created a standards-based method whereby IDS products and components can interoperate. The two end products of the IDWG are the Intrusion Detection Message Exchange Format (IDMEF) and the Intrusion Detection Exchange Protocol (IDXP). These specify the data format and exchange procedures, respectively. For further information, please refer to <http://www.ietf.org/ids.by.wg/idwg.html>.

**Table 4.16-3: IDS Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">ISS</a>	RealSecure Product suite	Network and host-based intrusion detection	Internet Gateway	ALL

**Table 4.16-4: IDS Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">ISS</a>	RealSecure Product suite	Network and host-based intrusion detection	Internet Gateway	ALL

#### 4.16.2 Authentication

Authentication is the process of verifying the identity of a user or entity to protect against unauthorized access to a system or to the information it contains. User authentication may be accomplished using various methods such as user ID, password, digital signature, biometrics devices, challenge response devices, smart cards, or token devices such as SecurID. The most common form is accounts and passwords. The weakness with this method is that passwords are often forgotten, stolen, or accidentally revealed. Authentication, regardless of the methods used, should be required once and should occur at logon – when signing on to the system or networks. The authentication information should then be kept for the rest of the session and passed as necessary to permit access to other applications and systems.

A security mechanism that can authenticate a user or entity, authorize access rights, and provide administrative capabilities is preferred. When used in a network environment, this mechanism will support authentication methods such as transmitting a name and password separately and in encrypted format, which reduces the possibility of compromise.

There are four types of authentication implementations currently: Kerberos, X.509, Distributing Computing Environment (DCE) (V1.2.1) security, and Secure European System for Applications in a Multi-Vendor Environment (SESAME). ISO 9798 is also an emerging international standard for entity authentication techniques.

- Kerberos (developed at the Massachusetts Institute of Technology [MIT] and named after the mythical three-headed dog that guarded Hades) provides network authentication based on a key distribution model. It allows entities communicating over networks to

prove their identities to each other while preventing eavesdropping or replay attacks. It also provides for data stream integrity and secrecy using cryptography systems, such as Data Encryption Standard (DES).

- X.509 is a certificate authorization service normally used for authenticating e-mail and electronic commerce clients and servers.
- DCE (v1.2.1) security is an implementation of Kerberos Version 5. DCE includes pre-authorization to inhibit password guessing attacks, authentication delegation, hierarchical trust, and General Security Service Application Programming Interfaces (GSSAPI) with extensions supporting Extended Registry Attributes. DCE (v1.2.2) supports the use of cryptocards and begins implementing Public Key technology. GSSAPI is an Internet standard specified in RFCs 1508 and 1509.
- Like Kerberos, SESAME Version 4 supports authentication without relying on externally produced code, thereby bypassing import restrictions. Kerberos client support is included as well as authentication delegation and GSSAPI support.

*Required Standards:*

- ISO 9798

#### **4.16.2.1 Authentication Protocols/Password Authentication Protocol**

Password Authentication Protocol (PAP) is a simple, clear text authentication scheme. The Network Authentication Server (NAS) requests the user name and password, and PAP returns them in clear text (unencrypted). This authentication scheme is not secure because a third party could capture the user's name and password and use it to get subsequent access to the NAS and all of the resources provided by the NAS. PAP provides no protection against replay attacks or remote client impersonation once the user's password is compromised.

**Challenge Handshake Authentication Protocol (CHAP – RFC1994)** – CHAP is an encrypted authentication mechanism that avoids transmission of the actual password on the connection. The NAS sends a challenge, which consists of a session ID and an arbitrary challenge string, to the remote client. The remote client must use the MD5 one-way hashing algorithm to return the user name and an encryption of the challenge, session ID, and the client's password. The user name is sent un-hashed.

**Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)** – MS-CHAP is a Microsoft version of the RSA Message Digest 4. It negotiates encryption and uses the RC4 algorithm to encrypt communications between host and client. MS-CHAP is the default Windows NT Remote Access Server (RAS) challenge and reply protocol.

*Required Standards:*

- RFC 1994 CHAP

**Table 4.16-5: Authentication Protocol Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Novell</a>	NDS	User profile (name, password and authorization)/LDAP authentication	Novell NetWare	Local
<a href="#">Novell</a>	Edirectory	User profile (name, password and authorization)/LDAP authentication	Novell NetWare	Local
<a href="#">Microsoft</a>	Active Directory	User profile (name, password and authorization)/LDAP authentication	Windows servers	Local

**Table 4.16-6: Authentication Protocol Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.16.2.2 Access Authentication Protocols

Remote Authentication Dial-In User Service (RADIUS) and Cisco's Terminal Access Controller Access Control System (TACACS+) are two prominent security protocols used to authenticate dial-up access into networks.

RADIUS is an access server authentication, authorization, and accounting protocol developed by Livingston Enterprises, Inc. It is a system of distributed security that secures remote access to networks and network services against unauthorized access.

RADIUS is comprised of three components:

- A protocol with a frame format that utilizes UDP/IP
- A server
- A client

The RADIUS server runs on a central computer typically at the customer's site, while the clients reside in the dial-up access servers and can be distributed throughout the network. The RADIUS server supports a variety of methods to authenticate a user. When it is provided with the user name and original password given by the user, it can support Point-to-Point Protocol (PPP), PAP, CHAP, UNIX login, and other authentication mechanisms.

- <http://www.ietf.org/rfc/rfc2865.txt>
- <http://www.ietf.org/rfc/rfc2869.txt>

[TACACS+](#) is Cisco's solution for remote access. Many features of RADIUS were included in the TACACS+ protocol.

**Table 4.16-7: Access Authentication Protocol Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	TACACS+	Remote access/dial-up Authentication	AO Dial-up	Local
<a href="#">Cisco</a>	RADIUS	Remote access/dial-up Authentication	VPN	ALL

**Table 4.16-8: Access Authentication Protocol Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	RADIUS	Authentication	All	ALL

### 4.16.3 Access Control

Access control is the process of determining whether a user or entity is authorized to use a system, network, or resource. Access control also deters attempts to gain unauthorized access. Access control authorization is the responsibility of the resource owner. The scope of access control can be extended to resources that span multiple domains.

Several access control methods currently employed in industry are described below:

- C2/DAC refers to the C2 security rating as established by the National Computer Security Center using Discretionary Access Control (DAC) concept.
- Distributed Computing Environment (DCE) authorization services are implemented using the Portable OS based on UNIX (POSIX) 1003.6 standard for Access Control Lists (ACLs).
- Role-based authorization is implemented using a combination of ACLs, user IDs, and group IDs.
- SESAME V4 implements authorization using the framework established by ITU-T in ISO 10181-3. The concept is similar to POSIX 1003.6.

Network-based access control is implemented on CISCO routers and firewall servers. There are many applications and operating systems that support role-based authorization.

*Required Standards:*

- POSIX 1003.6
- ISO 10181-3

**Table 4.16-9: Access Control Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	TACACS+	Remote access/dial-up Authentication	AO dial-up	Local
<a href="#">Cisco</a>	RADIUS	Remote access/dial-up Authentication	VPN	ALL
<a href="#">Novell</a>	NDS	User profile (name, password and authorization)/LDAP authentication	Novell NetWare	Local
<a href="#">Novell</a>	eDirectory	User profile (name, password and authorization)/LDAP authentication	Novell NetWare	Local
<a href="#">Microsoft</a>	Active Directory	User profile (name, password and authorization)/LDAP authentication	Windows servers	Local

**Table 4.16-10: Access Control Product Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Access control and authentication	ALL	ALL

#### 4.16.3.1 Password Usage

The password usage standard specifies basic security criteria for two different uses of passwords in an automated information system: personal identity authentication and data access authorization. A password used for personal identity authentication will be called a *personal* password; a password used for authorizing access will be called an *access* password. A personal password should not also be used as an access password. This document does not require the use of passwords in an automated information system for either purpose, but establishes the basic criteria for the design, implementation, and use of a password system in those systems where passwords are used. A password-based encryption algorithm is a secret-key algorithm in which the key is derived from a user-supplied password.

*Required Standards:*

- FIPS 112, Password Usage

**Table 4.16-11: Password Usage Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

**Table 4.16-12: Password Usage Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.16.4 Confidentiality, Integrity, and Non-Repudiation

Confidentiality ensures that any unauthorized entities or processes do not inadvertently access Judiciary-sensitive information. Typical methods of implementation are encryption and document classification.

Integrity is assurance that only authorized entities or processes have modified information. Any information that has been modified by unauthorized entities or processes will be detected, and the appropriate actions can be taken. Typical methods of implementation are physical message protection (seals and locks), encryption, digital signatures, and virus control.

Non-repudiation provides sufficient proof to the receiver of information that the sender is the originator of the information; the sender cannot deny sending the information. Encryption is a prerequisite for non-repudiation. A typical method of implementation is the receipt acknowledgement function within a message system. Public key non-repudiation solutions typically use digital signature.

#### **4.16.4.1 Encryption/Cryptography**

Encryption services provide the basis for confidentiality, integrity, and non-repudiation of information. DES and Rivest, Shamir, Adleman (RSA) are industry recognized standards. DES was developed in the 1970s by the National Bureau of Standards to provide a standard method for protecting sensitive commercial and unclassified data. With the help of the National Security Agency (NSA), DES officially became a federal standard in November 1976. RSA is ANSI standard X9.44. The NSA provides additional guidelines for Type 2 encryption techniques. Type 2 is a Government-approved encryption standard for unclassified information. In some cases DES is now deficient because of the processing power now available. A new algorithm was solicited by NIST and is called the Advanced Encryption Standard (AES). AES was approved as a standard in November 2001 and is FIPS 197.

Cryptography or data encryption is utilized in various applications and environments. In general, the cryptography is used to protect data from undetected modification, unauthorized usage or physical theft while it is being transmitted between two points or while it is stored in a medium. Cryptography is the technology that embodies mathematical algorithms for encrypting and decrypting binary coded information. The original message is called a plaintext. Encryption transforms the plaintext into some unreadable form, called a cipher-text, while decryption converts the cipher-text back into the plaintext. Currently there are two major approaches to data encryption: symmetric or secret-key cryptograph, and asymmetric or public-key cryptography. The major differences in these approaches is that a symmetric algorithm uses the same key for encryption and decryption, while a public-key algorithm uses one key (the public key) for encryption and another key (the private key) for decryption.

##### **4.16.4.1.1 Symmetric-key or Private-key Cryptography**

Symmetric or private-key cryptography is the technology in which encryption and decryption involve the same key, a secret key. Pairs of users share a secret key, keeping the key to themselves. Data encrypted with a secret key can be decrypted only with the same secret key.

The standards for symmetric, or secret-key, cryptography include:

- Data Encryption Standard (DES)
- Triple-DES (3DES)
- International Data Encryption Algorithm (IDEA)
- Password Usage

##### **4.16.4.1.2 Public-Key or Asymmetric Cryptography**

In the case of public-key cryptography, encryption and decryption involve different keys. The two keys are the public key and the private key, and either can encrypt or decrypt data. A user gives his or her public key to other users, keeping the private key to him or herself. Data encrypted with a public key can be decrypted only with the corresponding private key, and vice versa.

A public-key algorithm is an algorithm for encrypting or decrypting data with a public or private key. A private key is typically used to encrypt a message digest; in such an application, the private-key algorithm is called a message-digest encryption algorithm. A public key is typically used to encrypt a content-encryption key; in such an application, the public-key algorithm is called a key-encryption algorithm.

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from both Microsoft and Netscape. The corresponding technologies are part of existing or proposed Web, Internet, and computing standards.

The base of RSA is that each user has two keys, one private and one public, one decrypting what the other encrypted. The digital signature has some important security qualities, even though it does not provide privacy. A digital signature is a two-step process where messages are first run through a hashing algorithm to produce a representative digest. Much like a human fingerprint, the digest is unique and can be used to identify the document. The digest is in turn encrypted using the sender's private key. The digital signature actually has an advantage over a handwritten signature because it represents both the contents of the message and the author. To verify the signature, the recipient decrypts the signature using the public key of the sender. The decryption reveals the digest, which the recipient compares to his own computed digest. If the two digests are not identical, either the message was signed using an invalid private key, or someone tampered with the message. These security properties are called originator authentication and message integrity.

A mathematical algorithm is used to obtain the public and private keys. The algorithm involves multiplying two large prime numbers (a prime number is a number divisible only that number and the number one) and through additional operations deriving one set of numbers that constitutes the public key and another set that is the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and private keys are needed for encryption and decryption but only the owner of a private key ever needs to know that key. Using the RSA system, the private key never needs to be sent across the network or Internet.

*Required Standards:*

- RSA is ANSI Standard X9.44

#### **4.16.4.1.3 Data Encryption Standard**

The Data Encryption Standard (DES) algorithm is used to protect against unauthorized disclosure or undetected modification of unclassified information during data transmission or storage. FIPS 81, DES Modes of Operation, defines four modes of operation for the DES. The modes specify how data will be encrypted to ciphertext and decrypted to plaintext. This standard is for use with equipment and services requiring compliance with FIPS 46-3, DES.

DES encrypts data using a private (secret) key algorithm. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key. Data can be

converted from ciphertext back to plaintext only by using exactly the same key algorithm used to encipher it.

The Advanced Encryption Standard (AES) is defined to have key lengths of 128, 192, and 256 bits, as compared with the current 56-bit length of DES.

*Required Standards:*

- FIPS 46-3 Data Encryption Standard (DES) replaces FIPS 46-2 to recognize Triple DES
- ANSI X9.52 (Triple DES)
- ANSI X3.92-1981
- FIPS 81, DES Modes of Operation also ANSI3.106
- FIPS 197 Advanced Encryption Standard (AES)

#### **4.16.4.1.4 Triple-DES (3DES)**

The strength of encryption systems is determined by the length of the numerical key that is used to encrypt the information. Triple-DES (3DES) uses a key the same length as the current key, 56 bits, and encrypts the plaintext three times with three different keys. For each key, there are several possible ways of encrypting the data, known as modes. A number of modes of triple-encryption have been proposed:

- DES-EEE3: Three DES encryption with three different keys.
- DES-EDE3: Three DES operations in the sequence encrypt-decrypt-encrypt with three different keys.
- DES-EEE2 and DES-EDE2: Same as the previous format except that the first and third operations use the same key.

#### **4.16.4.2 Electronic Commerce Security Services**

Electronic commerce is the paperless exchange of business information. Technologies that could be used include Electronic Data Interchange (EDI), e-mail, Electronic Funds Transfer (EFT), or XML. Electronic commerce encompasses payment systems analogous to traditional credit cards and checks. Recently, the Internet has become the platform with the largest growth for electronic commerce. This growth has been fueled by the development of XML in particular. The most prominent protocols developed to provide security within Internet commerce or secure information exchange over the Internet are Secure Hypertext Transport Protocol (S-HTTP), Netscape's Secure Socket Layer (SSL), and VPN.

S-HTTP is an HTTP-based, message-related security enhancement developed by Enterprise Integration Technologies Corporation and endorsed by the W3C Consortium. S-HTTP takes each message, assigns a digital signature to it, encrypts it in an envelope, and sends it using a security protocol such as SSL. Because S-HTTP is an extension to HTTP, it is used primarily by web browsers.

The SSL protocol was developed by Netscape to provide channel security across TCP/IP using data encryption and reliability checks. SSL works on a network-transport level, establishing a

secure passageway, or tunnel, for traffic between a client (i.e., a browser) and server (i.e., a secure web server). All traffic within the tunnel is encrypted whether it needs to be or not.

#### 4.16.4.3 Virtual Private Network

Virtual Private Network (VPN) is designed to provide a secured channel between two network sites. After verification between the source and the destination site, information exchanged between the two sites is encrypted.

IP VPNs are managed or unmanaged Layer 3 (network or customer premises equipment (CPE)/edge-based) offerings. They provide a full range of Metropolitan-Area Network/Wide-Area Network (MAN/WAN) networking functionality using IP backbone transport technology — either a private carrier-operated network or shared public Internet IP network for a closed (or at least a well-defined) community of interest. IP VPN offerings take several architectural forms, depending on their intended use: remote access, internal enterprise networking (corporate intranets), or business-to-business networking (corporate extranets). Generally, managed IP VPNs deliver a common set of features: any-to-any connectivity, fault management, configuration management, security management, edge-device management, edge-to-edge Service-Level Agreements (SLAs), and possibly some project management/professional services. Features available will increasingly include management tools such as network/service operations monitoring/status reporting capabilities and even end-user controlled/dynamic bandwidth provisioning and service modifications (adds-deletes-changes) in a managed VPN environment. IP VPN types are varied and may include:

- Internet-based IP VPNs, typically using IP security (IPsec)
  - Multi Internet Service Provider (ISP) type – End-user managed or third-party managed
  - Single ISP type – End-user managed (with SLAs for transport), third-party managed or ISP managed (possibly with end-to-end SLAs)
- NonInternet-based IP VPNs (typically using Multiple-Protocol Label Switching -MPLS WAN)
  - End-user managed – Customer Premises Equipment (CPE) – Not typical
  - Service provider managed (CPE) – Fully meshed and multiple Classes Of Service (COS)

#### *Required Standards:*

- FIPS 140-1, Security Requirements for Cryptographic Modules

Figure 4.16-2 depicts the Standard US Courts VPN Configuration.

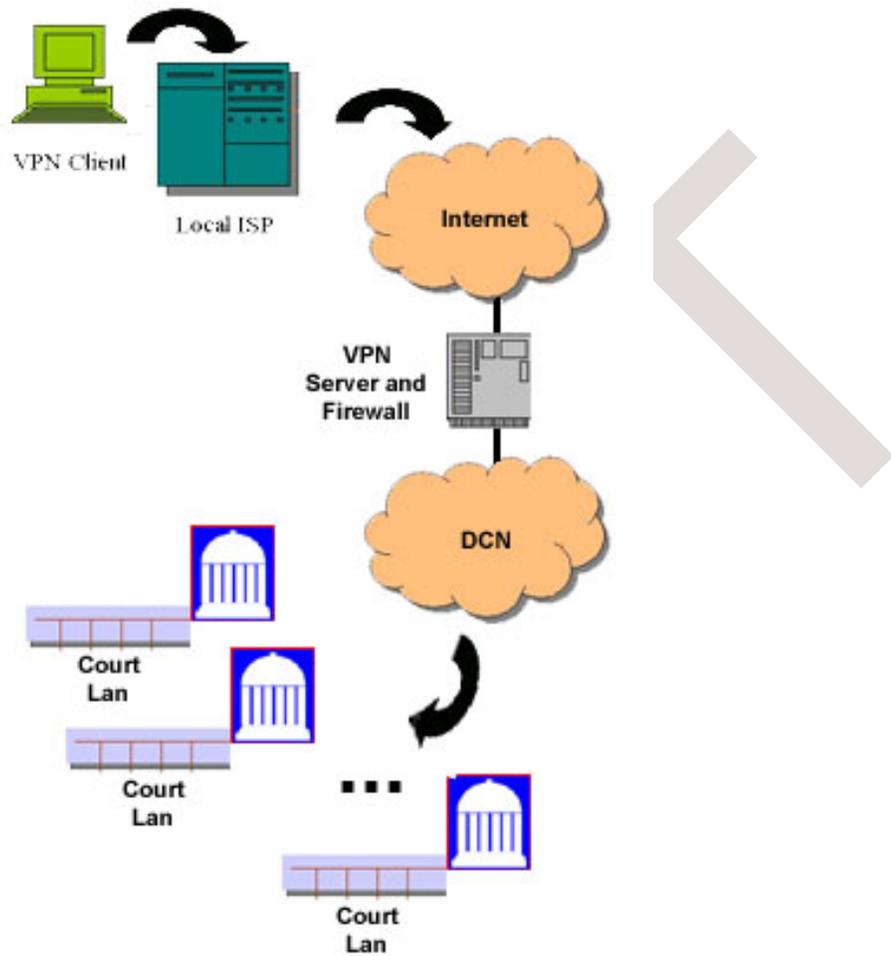


Figure 4.16-2: Standard US Courts VPN Configuration

Table 4.16-13: VPN Products Used by the Judiciary

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	Cisco VPN 3000 series hardware	Remote access Virtual Private Network (VPN) platforms and client software	Remote Access	ALL
<a href="#">Cisco</a>	Cisco VPN 3000 client	Remote access Virtual Private Network (VPN) client software	x86-based workstation	ALL

**Table 4.16-14: VPN Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	Cisco VPN 3000 series hardware	Remote access Virtual Private Network (VPN) platforms and client software	Remote Access	ALL
<a href="#">Cisco</a>	Cisco VPN 3000 client	Remote access Virtual Private Network (VPN) client software	x86-based workstation	ALL

#### 4.16.4.4 Virus Control

The number of computer viruses spreading around the world has increased dramatically. Some viruses just duplicate, others can cause serious damage or affect program and system performance.

Virus protection in a firewall is not very practical even with sophisticated packet filtering or proxy software. Some proxy server software may detect Java applications and provide warnings for the user before executing the applications. Although a firewall can scan all incoming traffic to determine whether it is allowed to pass through to the internal network, the scanning is mostly for source and destination addresses and port numbers, not for details of the data.

The most practical way to address the virus problem is through both host and client-based anti-virus software. For example, specialized host-based anti-virus software may be run at the SMTP gateway (e-mail server) and configured to perform scans of e-mail file attachments and automatically take corrective action. Additional host-based anti-virus software would be installed on all network file servers. Finally, each workstation should run client-based anti-virus software which always stays active in memory. In general, virus scanning software should be installed on all hosts and all clients, and configured to actively scan memory, boot sectors, and files being opened. Additionally, the software should be centrally administered and configured to ensure automatic updates of both the scanning engine and virus signature/definition files across the entire network.

Anti-virus software can aid in the removal of an infection, but can neither recognize nor determine the extent of damage. Furthermore, there can sometimes be a short delay between the release of new viruses and the availability of signature/definition file updates that recognize and combat the new release. Therefore, user education and regular system and data backups are vital.

**Table 4.16-15: Virus Control Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Symantec Corporation</a>	Norton AntiVirus	Server and workstation virus scan software	X86-based systems	ALL

**Table 4.16-16: Virus Control Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Symantec Corporation</a>	Norton AntiVirus	Server and workstation virus scan software	X86-based systems	ALL

#### 4.16.4.5 Public Key Infrastructure

A Public Key Infrastructure (PKI) is the set of hardware, software, policies, and procedures used to manage the public and private keys that provide the basis for several security services including authentication, integrity, non-repudiation, confidentiality, and access control. These security services are necessary and critical to the successful implementation of electronic commerce.

*Required Standards:*

- FIPS 140-1, Security Requirements for Cryptographic Modules
- The Internet Engineering Task Force (IETF) RFC 2144 - CAST, a symmetric key algorithm used within Entrust Product

##### 4.16.4.5.1 Digital Signature Standard

The Digital Signature Standard (DSS) offers a reliable and cost-effective way to verify that information has not been altered after it is signed, which helps to preserve message integrity.

A signature algorithm transforms a message of any length under a private key into a signature. By doing this, it is computationally infeasible to find two messages with the same signature, to find a message with a given, predetermined signature, or to find the signature of a given message without knowledge of the private key. Typically, a signature algorithm is implemented by computing a message digest on the message, then encrypting the message digest with the private key. The signature is then appended to the message and transmitted for verification by the receiver.

*Required Standards:*

- FIPS 186, Digital Signature Standard (DSS) (also Draft ANSI X9.30-199x Part 1; and ISO/IEC JTC1/SC27/WG2, Project 1.27.08 Digital Signature with Appendix)
- [FIPSPUB186-2](#) Digital Signature Standard (DSS), 2000 January 27

The DSS standard specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital, rather than written, signature. The DSA authenticates the integrity of the signed data and the identity of the signatory. The DSA may also be used to prove that data was actually signed by the generator of the signature. The DSA is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication. The DSA may be implemented in software, firmware, hardware, or any combination thereof.

#### 4.16.4.5.2 Digital Certificate Authentication (X.509)

Digital Certification Authorization (X.509) is the international standard for digital certificate authentication specially used for user identification, in the creation of electronic documents used to prove identity and public key ownership over a communications network. A digital certificate serves as an electronic credential that contains specific identifying information along with an individual's public key. It is a non-forgable, tamper-proof electronic document that attests to the binding of an individual's identity and his public key. To ensure that it has not been altered, the certificate must be signed by a trusted third-party individual or a Certificate Authority (CA). A third party can operate a CA, or an enterprise can self-certify its users and servers. The issued certificate or digital ID contains the subject name and public key from the self-signed certificate, and an issuer name, serial number, validity period, and signature algorithms of the CA's choice. Certificates can be extended with additional information. Once signed, certificates can be stored in X.500 directory servers, stored in other directory databases, transmitted over non-secure networks or distributed via any other means that make certificates easily accessible to users. Certificates are used until they expire or are revoked. A certificate may be limited to one-time use for certain types of transactions.

##### *Required Standards:*

- International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) (formerly called Consultative Committee on International Telephony and Telegraphy (CCITT) X.509, Certificate Authentication

**Table 4.16-17: X.509 Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Verisign	Verisign	X.509 certificates	x86-based systems	ALL

**Table 4.16-18: X.509 Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Verisign	Verisign	X.509 certificates	x86-based systems	ALL

#### 4.16.4.5.3 Digital Time Stamp

The digital time-stamp service or digital notary is a system that inserts a date and time in the text and binds a document to its creation at a particular time. The time stamp service uses a numbering scheme which makes it impossible to insert time stamps at a later time. Two features of a digital time-stamping system are particularly helpful in enhancing the integrity of a digital signature system: a time-stamping system cannot be compromised by the disclosure of a key; and the digital time stamp certificates can be renewed to remain valid indefinitely.

#### 4.16.4.5.4 Secure Hash Standard

The Secure Hash Standard (SHS) algorithm is used to verify a digital signature. The SHS specifies a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a

message or a data file. When a message is entered, the SHA-1 produces a 160-bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA), which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller than the message. The verifier of a digital signature must use the same hash algorithm that was used by the creator of the digital signature. The SHA-1 is called secure because it is computationally infeasible to find a message that corresponds to a given message digest or to find two different messages that produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify.

SHA-1 may be used with the DSA in electronic mail, electronic funds transfer, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication. The SHA-1 may also be used whenever it is necessary to generate a condensed version of a message. Although used primarily with DSA, it can be used in software distribution and data storage.

*Required Standards:*

- <http://www.itl.nist.gov/fipspubs/fip180-2.htm>- FIPS 180-2, *Secure Hash Standard (SHS)*, 2000 August, for SHA-1 Algorithm. SHA-1 is a technical revision of SHA (FIPS 180) <http://www.csrc.nist.gov/publications/fips/fips180-2.pdf>

#### **4.16.4.6 Security Protocols**

Cryptographic technology is embodied in industry-standard protocols such as SSL . These industry-standards protocols provide the foundation for a wide variety of security services, including encryption, digital signatures, message integrity check, and single-user logon. This section includes:

- Transport Layer Security (TLS)
- Secure Sockets Layer (SSL) Protocol
- Secure Multipurpose Internet Mail Extensions (S/MIME) Protocol
- Message-Digest Algorithms
- Audit
- Access Filtering, Monitoring, and Reporting

##### **4.16.4.6.1 Transport Layer Security**

The Transport Layer Security (TLS) Protocol provides communications privacy over the Internet by allowing client-server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The TLS protocol is based on the SSL 3.0 Protocol Specification as published by Netscape.

*Required Standards:*

- TLS Protocol Version 1.0, RFC 2246 (based on The Secure Sockets Layer (SSL version 3.0) - Internet Engineering Task Force [IETF]).

#### **4.16.4.6.2 Secure Sockets Layer**

Secure Sockets Layer (SSL) is an open, non-proprietary protocol designed by Netscape Communications for securing data communications across computer networks. SSL is sandwiched between the application protocol (such as HTTP, Telnet, FTP, NNTP) and the connection protocol (such as TCP/IP, UDP). SSL provides server authentication, message integrity, data encryption, and optional client authentication for TCP/IP connections. With the addition of SSL, data security can be achieved.

The primary goal of the SSL protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lower level, layered on top of a reliable transport protocol (e.g., TCP/IP), is the SSL Record Protocol. The SSL Record Protocol is used to encapsulate various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.

One advantage of SSL is that it is application protocol-independent. A higher level protocol can layer on top of the SSL protocol transparently. The SSL provides connection security that has three basic properties: (1) The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES, RC4, etc.). (2) The peers' identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS, etc.). (3) The connection is reliable. Message transport includes a message integrity check.

##### *Required Standards:*

- TLS Protocol Version 1.0, RFC 2246 (based on The Secure Sockets Layer (SSL version 3.0) - Internet Engineering Task Force (IETF))

#### **4.16.4.6.3 Secure Multipurpose Internet Mail Extensions (S/MIME)**

Public Key Cryptography Standard (PKCS) is a set of informal inter-vendor standards developed in 1991 by RSA laboratories. Since its publication, PKCS has been incorporated into several standards and products. PKCS describes the syntax for messages in an abstract manner, and gives complete details about algorithms. It does not specify how message is to be represented. Thus PKCS implementations are free to exchange messages in any manner, depending on character set, record size constraints, as long as the messages can be preserved from sender to recipient.

S/MIME relies on the Public Key Cryptography Standards (PKCS) to ensure cryptographic compatibility across vendors. MasterCard and Visa use S/MIME as the basis for the specification for securing online payment card transactions. S/MIME uses two simple cryptographic constructs: the digital signature and the digital envelope. Both are accomplished using RSA public key cryptography.

*Required Standards:*

- Public Key Cryptography Standard (PKCS) #7 - Cryptographic Message Syntax Standard
- RFC 3156: MIME Security with Open PGP
- [IP Authentication using Keyed MD5 \(RFC 1828\)](#)
- [The ESP DES-CBC Transform \(RFC 1829\)](#)
- [HMAC: Keyed-Hashing for Message Authentication \(RFC 2104\)](#)
- [HMAC-MD5 IP Authentication with Replay Prevention \(RFC 2085\)](#)
- [Security Architecture for the Internet Protocol \(RFC 2401\)](#)
- [The NULL Encryption Algorithm and Its Use With IPsec \(RFC 2410\)](#)
- [IP Security Document Roadmap \(RFC 2411\)](#)
- [IP Authentication Header \(RFC 2402\)](#)

#### **4.16.4.6.4 Message-Digest Algorithms**

A message-digest algorithm is a method of reducing a message of any length to a string of a fixed length, called the message digest, in such a way that it is computationally infeasible to find a collision (two messages with the same message digest) or to find a message with a given, predetermined message digest.

MD2 and MD5 are message-digest algorithms invented by RSA Laboratories. Each inputs an arbitrary message and outputs a 128-bit message digest.

*Required Standards:*

- RFC 1319: The MD2 Message-Digest Algorithm
- RFC 1321: The MD5 Message-Digest Algorithm

#### **4.16.4.6.5 Audit**

Audit services provide the authorized control and protection of the audit trail, the recording and dissemination of security-relevant events involving resources, and the management and inspection of the audit trail.

Security products that produce audit trails should be built to support continuous availability, configurable audit events, and electronic alarm reporting. Audit services also include tools that analyze and generate reports from the audit trail. When a security-relevant event occurs, the security audit service must generate an audit event that can be recorded, reported, archived, and analyzed.

The security products should generate audit records that are incorruptible and support the analysis and dissemination of audit records. In case of successful attacks on the firewall servers themselves, which may render the intruders full control of the firewall servers, the firewall audit records may have to be stored on a server other than the firewall to prevent the intruders from removing audit logs and hiding their trails.

#### **4.16.5 Access Filtering, Monitoring, and Reporting**

Access filtering is implemented using pass-through filtering technology. All HTTP requests for web pages pass through an Internet control point such as a firewall, proxy server, or caching device. Access filtering software is integrated with these control points and checks each request to determine whether it should be allowed or denied. The responses can be logged for reporting purposes. The filtering software works in conjunction with a master database of either prohibited or allowed URLs. Generally this master database is a subscription service, updated based on common criteria. Individual organizations subscribing to the service have the ability to add or remove addresses from the restricted list.

#### **4.16.6 Security Administration**

Security administration is the process of creating, maintaining, and monitoring security information such as access control policies, authorized user profiles, security parameters, and ownership identification. The resource owner, delegated custodian, or authorized groups perform this function. A security administrator must have the appropriate controls to ensure separation of duties from the system administrator or the group responsible for software installation and maintenance. The resource owner or persons responsible for maintaining the security information must ensure that the security data remains confidential.

#### **4.17 System and Network Management Services**

System and network management services ensure that the IT infrastructure continues to meet the Judiciary's growing information processing needs while sustaining and improving the quality, availability and efficiency of all Judiciary IT services. System and network management services enable the Judiciary to adopt an integrated and proactive management approach to managing its critically important IT components, and enables end-to-end delivery of IT services in accordance with service level requirements (agreements), even as the Judiciary continues to enhance its computing environment.

System and Network Management Services include the following areas:

- Network System Administration
- Help Desk Administration
- Communication Network Management
- Server Management
- Capacity Planning and Performance Management
- Backup and Recovery Service

Simple Network Management Protocol (SNMP) is the standard operations and maintenance protocol. Server management uses this protocol to communicate over other protocols, such as TCP/IP, IPX, and UDP. SNMP provides a means of obtaining information from, and sending information to, network devices. SNMP is based on the manager-agent model, and uses Management Information Bases (MIBs) to exchange information.

### 4.17.1 Network System Administration

Network system administration provides tools for hardware and software asset inventory, software distribution and installation, and remote diagnostics to better manage the computing environment on a network of any size, be it a few machines or tens of thousands of desktops. The tools are designed to help systems administrators install and maintain operating systems and applications, discover system configurations, and perform help desk operations. The tools integrate with the major enterprise management solutions.

An asset inventory tool is used to automatically discover and track hundreds of asset elements, including installed hardware, software, configuration files, serial numbers, TCP/IP addresses, e-mail addresses, user logon IDs, etc. The tool needs to provide scalable support for various platforms (Windows, NetWare, Linux, etc.), and employ an open database for ease of integration, historical reporting, and analysis.

A software distribution tool is used by help desk administrators or system administrators to update the legacy applications, post system updates and bug fixes, repair broken desktop programs (adding new files or replacing missing or corrupt files), and update operating systems across a mix of technology platforms. It also ensures consistent versions of software applications throughout an enterprise.

A remote diagnostics tool assists the system administrators and help desk administrators in performing online remote troubleshooting.

*Required Standards:*

- Reference Operating Systems Services Standards
- Reference Network Services Standards

**Table 4.17-1: Network System Administration Products Used by the Judiciary**

<b>Vendor</b>	<b>Product</b>	<b>Function</b>	<b>Judiciary Platform</b>	<b>Scope</b>
<a href="#">Bindview Inc.</a>	Bindview management tool	Audit tool	x86-based workstation	Local
<a href="#">Hewlett Packard</a>	Download Manager	Update firmware on HP JetDirect print servers.	x86-based workstation	Local
<a href="#">Hewlett Packard</a>	JetAdmin	Manage and configure network printers (HP JetDirect print servers)	x86-based workstation	Local
<a href="#">Novell</a>	Zenworks 2.0	System Management, including distributing software	x86-based workstation	Local
<a href="#">Symantec</a>	Ghost	Re-image workstation configuration	x86-based workstation	Local

**Table 4.17-2: Network System Administration Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		System Management, including distributing software	ALL	

#### 4.17.2 Help Desk Administration

The help desk is the primary point of contact for IT problems and service requests, and is responsible for managing desktops, performing trend analysis and reporting, initiating proactive support, minimizing calls, and responding to system outages. Help desk administrators typically receive problem and service requests from users via phone, voice mail or e-mail, then log information into the call management system and perform troubleshooting. In troubleshooting, help desk technicians shall use the following information sources:

- Remote diagnostics tool, (online troubleshooting tools).
- Knowledge management system to search for “known error” to resolve problems.

Help desk functionality includes Root Cause Analysis (RCA) procedures to determine the cause of the outage or loss of major functionality, resolve the problem, and restore service to the customers. Reactive help desk management occurs when the help desk is not aware of a problem until reported by a customer or an IT operations activity, such as network management. Conversely, to be proactive and minimize support calls, operations management technologies for IT operations management (e.g., HP OpenView’s Network Node Manager (NNM) and IT/Operations) should be deployed to generate trouble tickets for IT event/alarm thresholds and notify IT staff to repair the problem.

Network and specialized help desk management tools minimize the time needed to service the end-user at the desktop through remote access and functions, providing visibility and tracking, and trend analysis of logged problems and previously identified solutions. Help desk management also includes change scheduling procedures and a change management tool for tracking and supporting requests, IT modifications, and hardware or software repair and replacement.

Required Standards:

- Reference Section 4.3, Operating Systems Services Standards
- Reference Section 4.11, Network Services Standards

**Table 4.17-3: Help Desk Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
USInfoTel	<u>HEAT</u>	Help desk tool which supports remote location help desk operation, operations status, reports	x86-based system	ALL

**Table 4.17-4: Preferred Help Desk Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Help desk tool which supports remote location help desk operation, operations status, reports	x86-based system	ALL

### 4.17.3 Communication Network Management

The Judiciary network infrastructure consists primarily of a switched Ethernet architecture. The network infrastructure is interconnected via routers with T-1 and DS-3 links. The T-1 and DS-3 links are connected to routers in each of the Judiciary buildings. Networks (subnets) at individual locations are primarily 100 Mbps Fast Ethernet.

Network management tools provide a single point of control to manage multiple network systems. The primary interface is a consolidated graphical representation of the network. Network management consists of the following operational activities:

- Network fault management
- Network configuration management
- Network performance management

In order to be successful, network management must be proactive rather than reactive (e.g., only monitoring whether network devices are up or down). Proactive network management consists of the following steps:

1. Finding out the current state of the network - what devices are present, how they are configured, how they are behaving, what the performance levels are, what is currently going wrong.
2. Identifying trends and determining how to optimize the network by changing configurations, replacing network devices, etc.
3. Predicting what might go wrong, determining how to prevent it, and learning to avoid future problems.

For the network information to be up-to-date, the network management system must continually identify the current state of the networks/subnets (e.g. up, down, or marginal), network topology changes, including the discovery of the new/removed nodes, and configuration changes. Thresholds for the critical network devices must be configured and the system should notify staff when anything goes wrong. For example, thresholds can be set to monitor CPU loads, disk space used, interface and link errors and collected MIB data.

Network performance management measures the performance of network hardware, software, and media, such as throughput rate, percentage utilization, error rates and response time, through the collection and analysis of data about the network.

SNMP is the standard management protocol and is used to communicate over other protocols, such as TCP/IP, IPX, and UDP. SNMP provides a means of obtaining information from, and sending information to, network devices. SNMP is based on the manager-agent model, and uses MIBs to exchange information between them.

*Required Standards:*

- Network Services standards
- SNMP (Simple Network Management Protocol)

**Table 4.17-5: Network Management Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	CiscoWorks	Enterprise mapping, configuration, backup, and deployment of software to routers and switches		ALL
<a href="#">Ipswitch Inc.</a>	Whatsup Gold	Network performance and problem monitoring, mapping	x86-based workstations	ALL
<a href="#">Hewlett Packard</a>	HP Open View	Fault management, high-level configuration management, and performance management		ALL
<a href="#">MRTG</a>	Multi Router Traffic Grapher (MRTG)	Monitoring the traffic load on network		ALL

**Table 4.17-6: Network Management Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
	TBD	Enterprise mapping, configuration, backup, and deployment of software to routers and switches		ALL
	TBD	Network performance and problem monitoring, mapping	x86-based workstations	ALL
	TBD	Fault management, high level configuration management, and performance management		ALL
	TBD	Monitoring the traffic load on network		ALL

#### 4.17.4 Server Management

Server management activities are responsible for providing expertise in installing, configuring, and managing server, operating system, and data storage systems. Operational activities include troubleshooting and resolving operating system and related software problems, establishing and monitoring performance, availability and Application Information System (AIS) service-level agreements; and providing technical expertise to AIS developers. The objective of server management is to address the needs of each AIS for:

- Hours of availability
- Hours of support
- Availability and redundancy
- Performance (Key Volume Indicator) metrics

Server management must be proactive and corrective actions should be automated and configured to monitor the application’s availability and performance and/or to notify the appropriate Judiciary staff through paging or e-mail when something goes wrong.

*Required Standards:*

- SNMP (Simple Network Management Protocol).

**Table 4.17-7: Server Management Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Hewlett Packard</a>	HP Open View	Efficient event management, with customizable event filtering and consolidation	Sun Solaris server	
<a href="#">Ipswitch Inc.</a>	Whatsup Gold	Network performance and problem monitoring, mapping	x86-based server	

**Table 4.17-8: Server Management Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Fault management process and workflow, efficient event management, with customizable event filtering and consolidation	x86-based server	ALL

#### 4.17.5 Capacity Planning and Performance Management

Capacity planning and performance analysis provides computer and network performance analysis information used for planning new hardware acquisitions and for allocating the IT

resources needed to maintain business application performance levels. When linked to business performance, IT performance analysis information is used to avoid potential capacity problems, and bring potential performance problems to light before they happen, in a way that is meaningful to the business area.

Capacity planning and performance management applies capacity modeling technology to a particular database/repository to understand how current capacity is used (down to a service and component level), strategically allocate IT resources before capacity bottlenecks impact operations, and support the planning of service levels and investment strategies. Capacity planning and performance management needs to provide the following activities:

- Automatically collect and perform trend analysis of end-to-end performance and availability metrics (i.e., from network, network devices, server, application and database) and denote when thresholds are exceeded and outages occur in the collected data.
- Provide the collected data to a central point (e.g. a capacity management database / repository) and link the data with related information, such as configuration, service level, cost, and business forecast information.

*Required Standards: N/A*

**Table 4.17-9: Capacity Planning/Performance Management Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Web Trends</a> (subsidiary of NetIQ)	Web Trends Enterprise	Web statistical analysis tool	ISun Solaris Server	Jnet

**Table 4.17-10: Capacity Planning/Performance Management Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Web statistical analysis tool	x86-based server	ALL

#### 4.17.6 Backup and Recovery Service

Backup and recovery services are an important component of an enterprise services availability strategy. The development and management of a sound backup and recovery strategy at the Judiciary is a difficult task due to the generally distributed nature of judiciary services. In distributed computing environments, backup and recovery requirements are often best addressed by using two different methods – one for handling the relatively static data of the execution environment (e.g. operating systems and applications), and another for handling the dynamic data of the transaction environment (e.g., database tables and logs).

If the operating system and application data are co-located on a swappable (either physically or logically) device(s), then fast and reliable backup and recovery of the execution environment can be accomplished by the creation of an exact image copy of the device. Techniques available for the creation of these types of copies include bootable backup utilities, disk mirroring, and volume copy utilities. Backup is required only after a change in OS or application configuration.

Backup of transaction data in a distributed computing environment is best handled by an enterprise backup tool that is designed to work with the specific applications that make up the transaction environment. These are used in conjunction with high-performance storage subsystems. Under this configuration, all transaction systems are simultaneously accessed. Working copies (snapshots) of all transaction volumes are made across high-speed internal buses of the storage subsystem. The transaction systems are restarted, and backup is performed from the working copies. After backup is complete, the working copies are retained between backups for use as immediate recovery volumes.

The help desk provides the services to resolve desktop workstation problems. One of problems is the file(s) that are accidentally deleted or corrupted. Help desk administrators need data file recovery and undelete utilities to in order to rescue files and avoid having to rebuild entire desktop systems.

**Table 4.17-11: Backup Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Veritas</a>	BackupExec	Backup and recovery for individual Novell NetWare and Microsoft NT/2000 servers	X86-based servers	ALL
IBM/Tivoli	Tivoli Storage Manager (TSM)	Backup and recovery for individual Novell NetWare and Microsoft NT/2000 servers	x86 and mainframe	AO
CA	ARCserve	Backup and recovery for individual Novell NetWare and Microsoft NT/2000 servers	x86 Linux	CM/ECF

**Table 4.17-12: Backup Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
Veritas	BackupExec	Backup and recovery for individual Novell NetWare, Microsoft NT / 2003, and Linux servers	x86-based servers	ALL

#### 4.18 Distributed Computing Services

Distributed computing services provide specialized support for applications that may be physically or logically dispersed among computer systems in a network, yet wish to maintain a cooperative processing environment. A distributed network spreads individual services and isolated pieces of data across multiple networked machines. Information and services become transparently available because location-specific references are removed. This makes a network logically centralized and physically distributed.

Distributed computing services include:

- Distributed Computing Application Services
- Three-Tier Web-enabled DCA Model
- Distributed Computing Architecture Framework
- Internet/Extranet Architecture Option
- Intranet Architecture Option
- Overview of DCAF Standards and Functional Elements
- Online Transactional Processing (OLTP)
- Distributed Computing Application Security
- Message Queuing
- Web Services

Distributed computing services is a preferred architecture for the judiciary (whether physically or centralized or distributed). The following sections provide a general outline and vocabulary for discussing distributed computing services.

#### 4.18.1 Distributed Computing Application Services

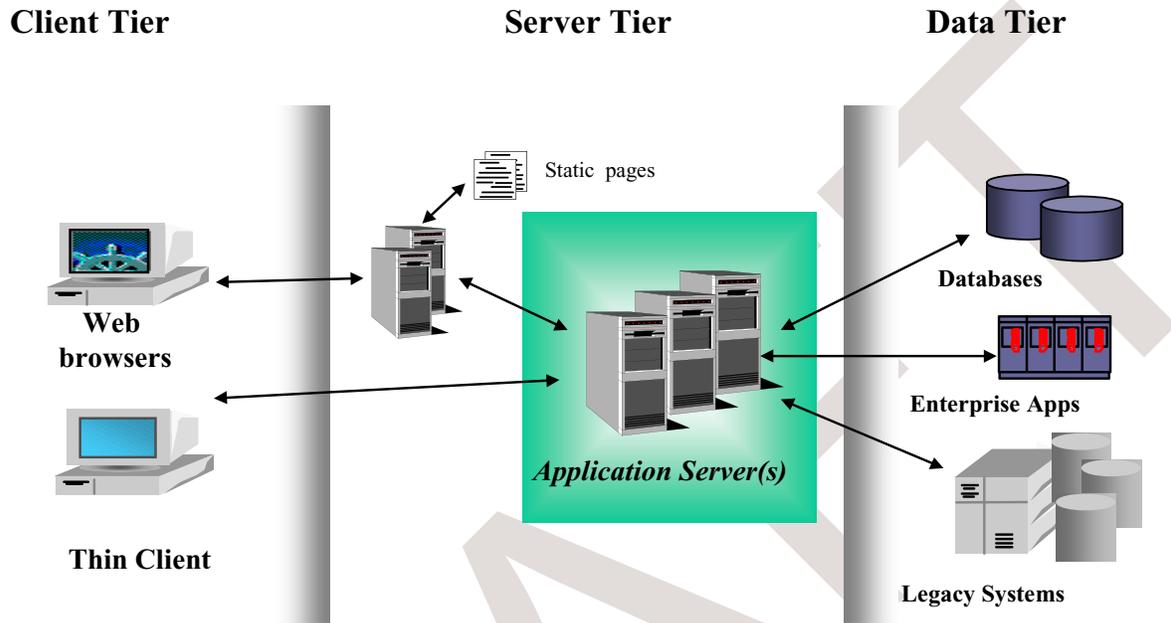
The foundation for distributed computing applications is the multi-tier concept. An application model is the conceptual division of a software application into functional components. The following table shows the generic 3-tier Application Model of Distributed Systems.

**Table 4.18-1: Generic 3-Tier Distributed Systems Application Model**

Functional Tier	Layer View	Layer Function
Presentation	Graphic Layout	Graphic User Interface (GUI)
	Presentation Logic	The logic that manage screen formats, screen content, and the interaction with the user.
Business Logic	Business Logic	Application functions that deal with business logic and the flow of control among application components. Business rules can be enforced here.
Data Access	Data Logic	The logic that relates to the storage and retrieval of data and the enforcing of business rules about data consistency.
	Database Management	The storage, retrieval, management, and recovery of data.

### 4.18.2 Three-Tier Web-enabled DCA Model

The model may be applied to any application but is illustrated below for web-enabled applications.



**Figure 4.18-1: Physical View of the Generic 3-Tier Web-Enabled DCA Model**

Based-on the framework described above; there are two functional mappings to the same physical model: the current model and the future model. Figure 4.18-2 depicts the functional and physical mapping to the current model. Figure 4.18-2 depicts the mapping to the future model using J2EE.

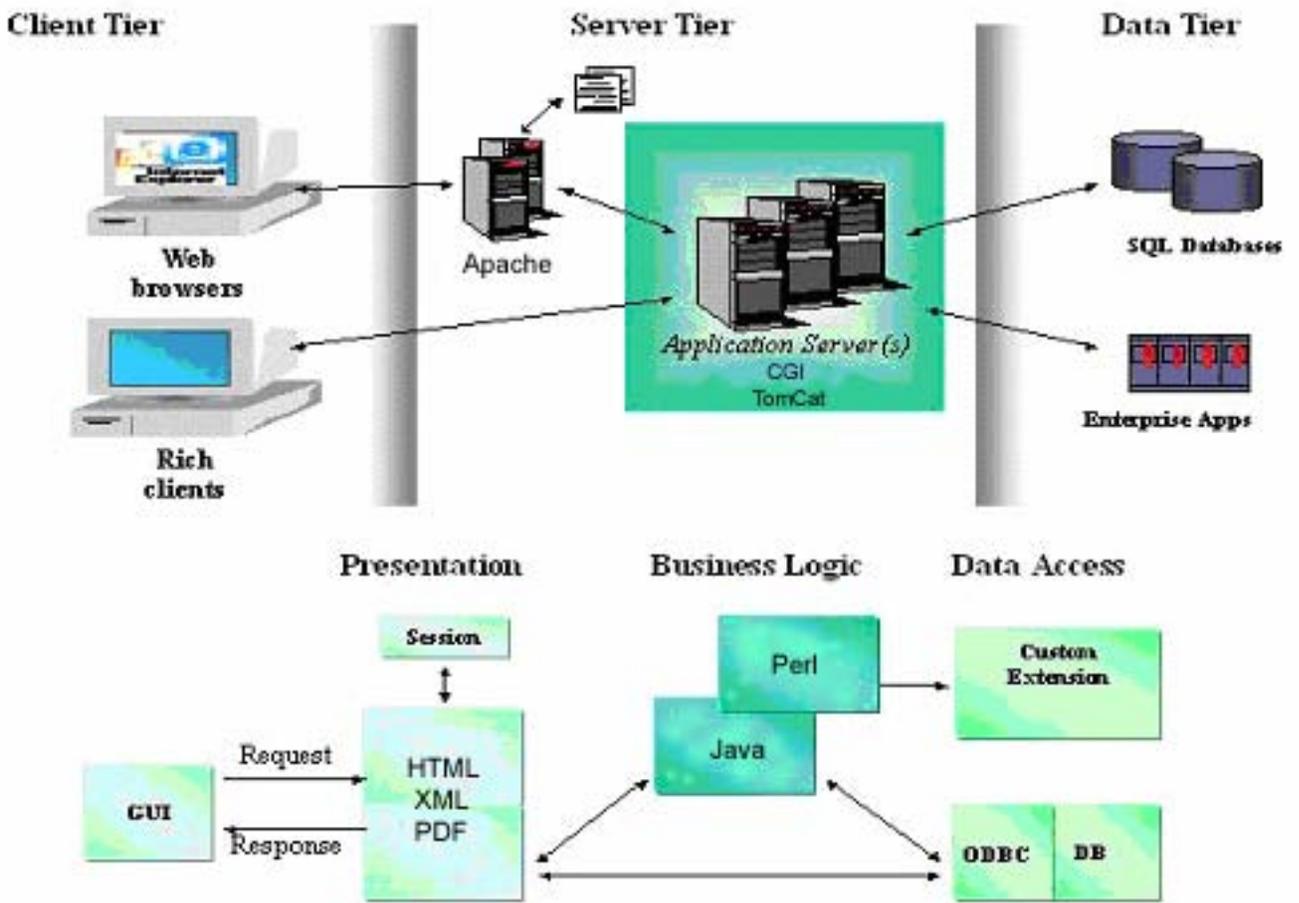


Figure 4.18-2: Current Functional and Physical Mapping

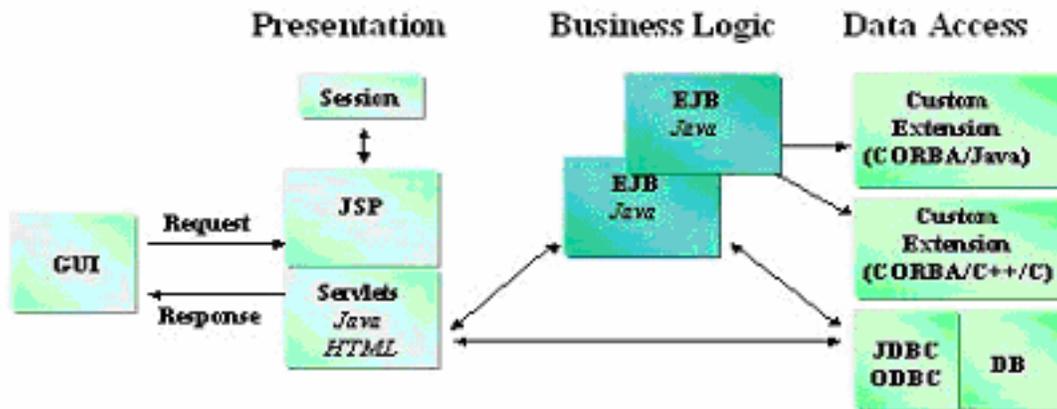
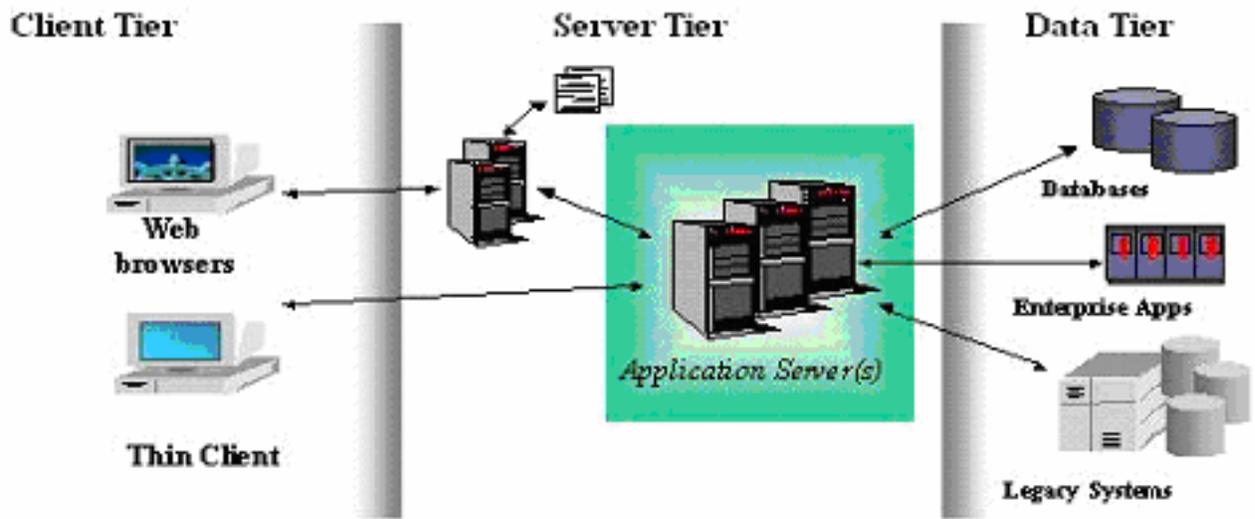


Figure 4.18-3: J2EE Future Functional and Physical Mapping

### 4.18.3 Distributed Computing Architecture Framework<sup>1</sup>

Although often referred to indistinguishable from one another, a Distributed Computing Architecture is broader than the Distributed Computing Applications Architecture (DCAA). A Distributed Computing Architecture is critical not only to solve application problems (e.g., performance, scalability) and implement E-commerce, but also to implement Enterprise infrastructure service solutions (e.g., clustering-failover, backup-recovery, security and storage).

The Judiciary applies the concept of a Distributed Computing Architecture Framework (DCAF) to simplify the view of Distributed Computing Services which are the foundation for distributed application development and integration, and to ensure consistency and focus on integration and interoperability.

The Judiciary DCAF is used to illustrate Distributed Computing Services in the context of the related TRM service areas and to define a subset of distributed computing services integrated with TRM standards and products.

---

#### <sup>1</sup> References:

- a. J2EE Technology in Practice, Building Business Applications with the Java 2 Platform, Enterprise Edition, Rick Cattell, Jim Inscore and Enterprise Partners. Addison-Wesley, June 2001.
- b. Designing Enterprise Applications with the Java 2 Platform, Enterprise Edition. N. Kassem and Enterprise Team. Addison-Wesley, 2000.
- c. Core J2EE Patterns, Best Practices and Design Strategies, Prentice Hall PTR, 2001.
- d. Applying Enterprise JavaBeans, Component-Based Development for the J2EE Platform, Addison-Wesley, 2001.
- e. "CORBA 3 Fundamentals and Programming", published by John Wiley.
- f. 3-Tier Client/Server At Work, Jeri Edwards, John Wiley, 1999.
- g. Core Servlets and JavaServer Pages, Marty Hall, Prentice Hall, 2000.
- h. Enterprise Application Integration, David Linthicum, Addison-Wesley, 2000.
- i. iPlanet Application Server 6.0 White Paper, Technical Reference Guide, 2000.
- j. XML Technology, Sun, <http://www.sun.com/xml>, 2001.
- k. C# and the .Net Platform, Andrew Troelsen, Apress. 2001.
- l. For more information on J2EE, refer to <http://developer.java.sun.com/developer/infodocs/>.
- m. For more information on .Net, refer to <http://www.microsoft.com/mspress/default.asp>

Distributed Computing Architecture Framework (DCAF)	Distributed Computing Application Architecture (DCAA)	DCAA Elements	
		Browser	
		Web Server	
		Web Application Server Middleware	
		Application Development Standard	
		Transaction Middleware	
		Other Middleware	
		Database Management & Legacy systems	
		Application Level Security	
		Protocol between client and server	
		Server OS	
	Data Distribution and Administration Architecture		
	Storage Architecture		
	Network Architecture		
Enterprise Security Architecture			
Enterprise Availability Backup and Recovery Architecture			
Enterprise Management System Architecture (EMS)			

**Figure 4.18-4: Distributed Computing Architecture Framework (DCAF)**

The multi-tiered Distributed Computing Applications Architecture (DCAA) model is the shaded element of the DCAF.

The DCAA is the one key element where Architecture Framework Options are applied, as depicted in Figure 4.18-5.

Distributed Computing Architecture (DCA)	Distributed Computing Application Architecture (DCAA)	DCAA	Class 1 and Class 2	Class 2 (only)	Class 3
		Browser	Internet Explorer and Netscape Browser		
		Web Server	Apache/Tomcat	Apache	Apache
		Web Application Server Middleware	J2EE-compliant Weblogic	ASP, Coldfusion MX	Open Source CMS
		Web Application Programming Language	J2EE, C++	C++, VB	Perl PHP
		Enterprise Middleware	TPM: J2EE application Server Weblogic	TPM: MTS	mod_perl PHPaccelerator
		Database Management	Informix	Microsoft SQL Server	MySQL
		Application Level Security	JNDI, ACLs, PKI, LDAP, Resource Gateway	PKI, LDAP, ACLs	JNDI, ACLs, Encrypt PKI, LDAP, Virtual Vault?
		Protocol between client and server	Internet/Extranet: HTTP(S)/SOAP Intranet: HTTP(S), IIOP, RMI, SOAP	COM/COM+/DCOM/SOAP	HTTP(S), CORBA, SOAP, UDDI, XML
		Server OS	Linux	Windows 2003 Server	Linux
Data Distribution and Administration Architecture					
Storage Architecture					SAN, Cluster File System
Network Architecture					
Enterprise Security Architecture					Tools to integrate with PKI, Resource Gateway?
Enterprise Availability Backup and Recovery Architecture					
Enterprise Management System Architecture (EMS)					

**Figure 4.18-5: DCA Framework with Options**

The Architecture Framework Options, labeled Class 1, Class 2, and Class 3, define an alternative set of standards and/or products to satisfy functions of the DCAA part of the DCAF depending on the deployment environment. Different business, operation, security requirements and technologies determine the different options described in the framework.

Architecture Framework Class 1 is for AISs with requirements to serve large volumes of users, transactions, data (and therefore distributed computing and enterprise-level storage infrastructure) *or* Extra/Internet access (and therefore associated security constraints and W3C standards) *or* enterprise-level service requirements (e.g., backup recovery).

Architecture Framework Class 2 is for AISs which are departmentally based, with requirements for small volumes *and* Intranet access.

Architecture Framework Class 3 is for a Target Technology Evolution “Pilot” AIS where the risk (schedule, scope, cost) is acceptable given that the AIS serves as the proving ground for new technologies, especially the migration to emerging technology trends such as web portal and web services (e.g., Universal Description Discovery Integration [UDDI], Simple Object Access Protocol [SOAP], etc.).

The remaining DCAF components are based on consistent enterprise architecture standards and products that apply to both Class 1 and Class 2, and so are not detailed in this section. They are defined in their respective TRM service areas.

The Class 3 Option is illustrated with a projected subset of pilot standards and products in order to provide an informational context with respect to future architecture direction. Class 3 lists potential standards and products which may become preferred given technology evolution and current information. For example, Class 3 may apply to those applications which are pilots for a new technology such as web portal server, SOAP<sup>1</sup>, or UDDI specification<sup>2</sup>. Class 3 standards and/or products are not to be confused with currently approved TRM preferred standards and products.

#### 4.18.4 Internet/Extranet Architecture Option

Figure 4.18-6 shows the Class 1 Option DCAA in the context of the overall target DCA.

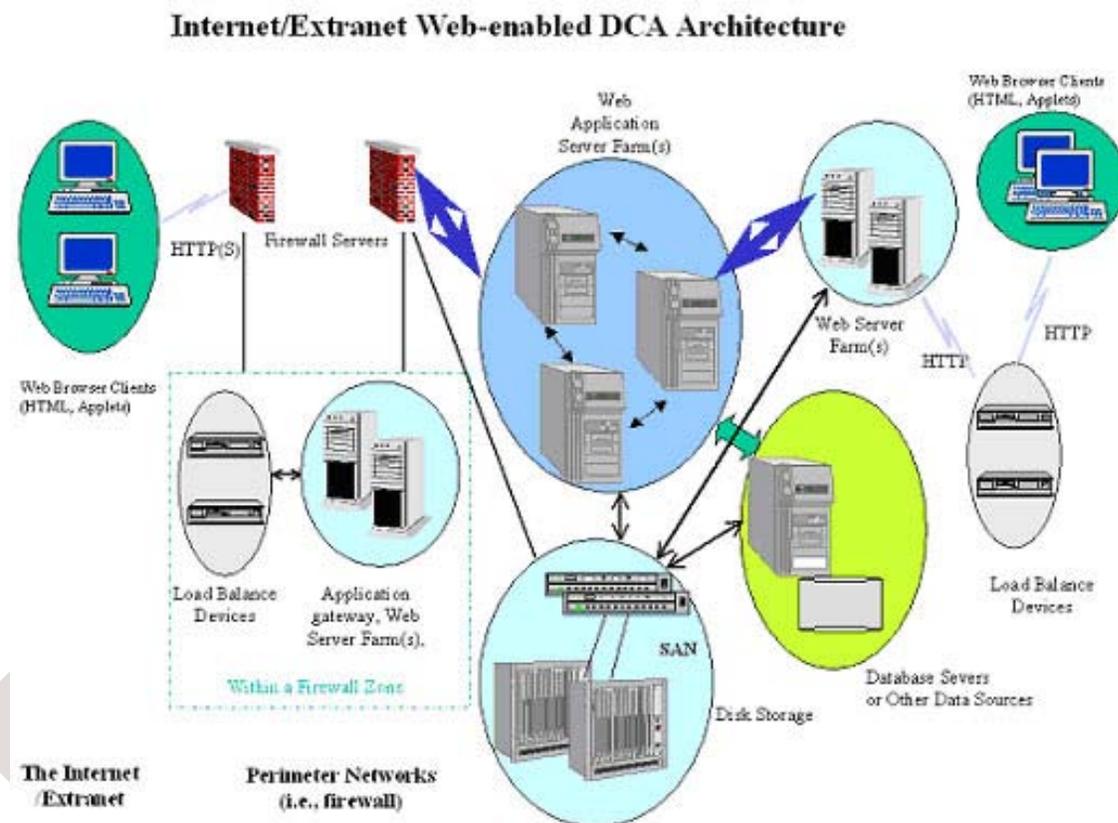


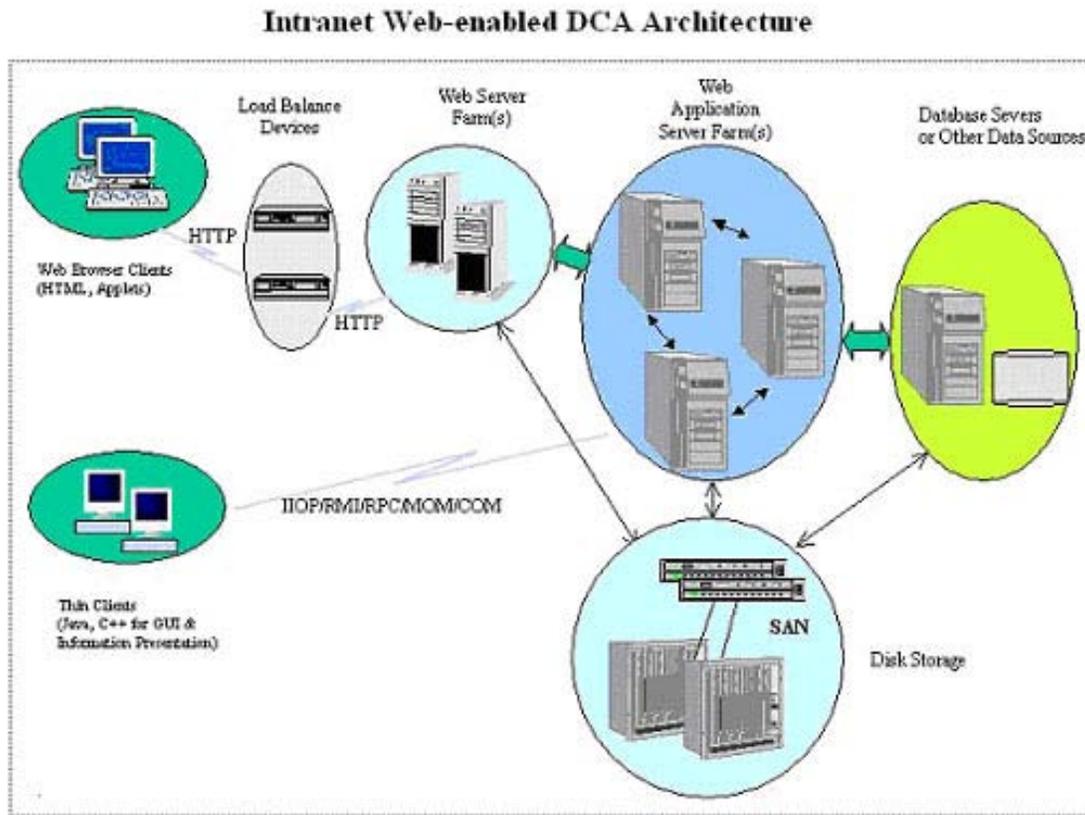
Figure 4.18-6: Class 1 Option Architecture Framework

<sup>1</sup> Reference World Wide Web Consortium home of Web Services Description Languages and SOAP specifications, <http://www.w3.org>

<sup>2</sup> Reference <http://www.uddi.org>

#### 4.18.5 Intranet Architecture Option

Figure 4.18-7 shows the Class 2 Option DCAA in the context of the overall DCA.



**Figure 4.18-7: Class 2 Option Architecture Framework**

The following sections provide more background on the overall DCAF concept and the DCAA elements of the DCAF in particular.

#### 4.18.6 Overview of DCAF Standards and Functional Elements

Object Transaction Monitor (OTM) is a term used to describe the distributed object application server and its associated functions. OTM represents the convergence of two technologies – traditional Transaction Processing Monitors (TP Monitor), such as BEA System's Tuxedo product, and distributed object services such as Object Request Brokers (ORBs) based on Common Object Request Broker Architecture (CORBA). OTMs combine the functions of traditional TP Monitors and ORBs. An OTM provides a component-based environment and automatically manages the most complex aspects of enterprise computing such as object brokering, transaction management, security, persistence and concurrency.

There are two industry standards for OTMs: Enterprise Java Beans (EJBs), and CORBA Beans. The EJB standard was a joint effort by a number of companies including Sun, Oracle, IBM, BEA, Netscape, Inprise, Gemstone, Sybase and others. EJB is a part of the Java™ 2 Platform, Enterprise Edition (J2EE) standard. The Object Management Group (OMG) is defining a multi-language EJB, called CORBA Beans, as part of the CORBA 3.0 standard.

J2EE provides a standard for developing multi-tier enterprise applications. J2EE simplifies enterprise applications by basing them on standardized, modular components, by providing a complete set of services to those components, and by handling many details of application behavior automatically, without complex programming.

J2EE includes many features of the Java 2 Platform, Standard Edition, such as "Write Once, Run Anywhere" portability, JDBC API for database access, CORBA technology for interaction with existing enterprise resources, and a security model that protects data even in internet applications. Building on this base, J2EE adds full support for Enterprise JavaBeans Components, Java Servlets API, JavaServer Pages, and XML technology. The J2EE standard includes complete specifications and compliance tests to ensure portability of applications across the wide range of existing enterprise systems capable of supporting J2EE. The most important components are:

- A Java servlet is a server-side application component, a Java object that is an instance of the Servlet class. The Servlet class is among the code defined in the Servlet API specification.
- A JavaServer Page (JSP) is a template for presenting dynamically generated Web content. JSPs are text files written in a combination of standard HTML tags, JSP tags, and Java code.
- Enterprise JavaBeans is a component model for developing and deploying Java applications in a multi-tiered, distributed architecture.
- The JDBC API is a standards-based set of classes and interfaces that enable developers to create data-aware EJBs. It is the API for accessing relational data from Java.

Other components include Java Naming & Directory Interface (JNDI), Java IDL/RMI over Internet Inter-Orb Protocol (IIOP) (CORBA interoperability), Java Messaging Services (JMS), Java Transaction API (JTA), Java Mail, and Java APIs for XML (JAXP, JAXM, JAX\_RPC etc.). JNDI is the API for accessing information in enterprise name and directory services. Java IDL is the API for calling CORBA services. JMS is the API for sending and receiving messages via enterprise messaging systems like IBM's MQ series. JTA is the API for managing and coordinating transactions across heterogeneous enterprise information systems. JavaMail is the API for sending and receiving e-mail. JAXP is the Java API for XML processing, JAXM is the Java API for XML messaging and JAX\_RPC is the Java API for XML-based RPC.

Figure 4.18-8 shows the J2EE container-based component management model, or J2EE framework. Figure 4.18-9 depicts the web application server framework.

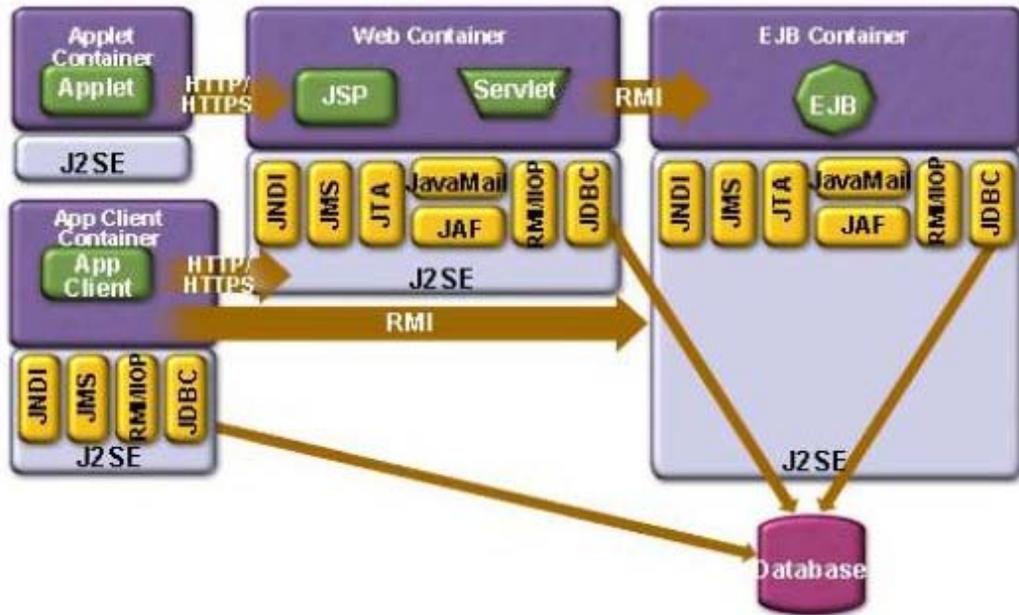


Figure 4.18-8: J2EE Container-Based Component Management Model

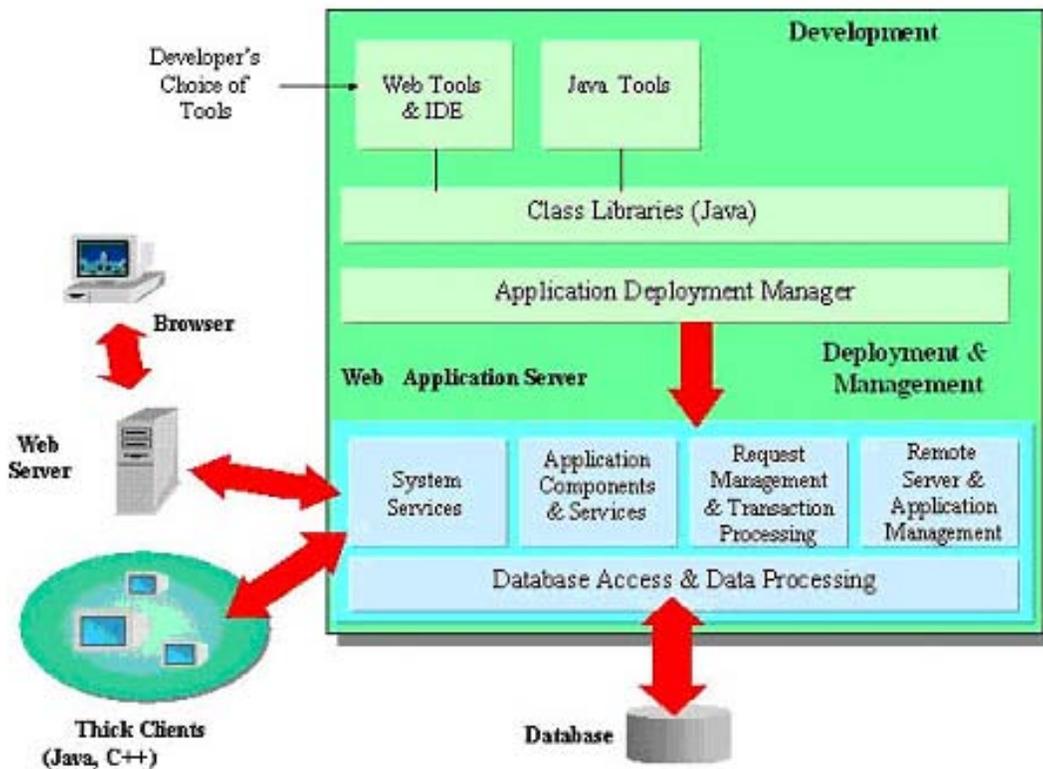


Figure 4.18-9: Web Application Server Framework

CORBA is the acronym for Common Object Request Broker Architecture. CORBA is the Object Management Group's (OMG's) open, vendor-independent, specification for an architecture and infrastructure that computer applications use to work together over networks. Interoperability results from two key parts of the specification: OMG Interface Definition Language (OMG IDL), and the standardized protocols General Inter-Orb Protocol (GIOP) and Internet Inter-Orb Protocol (IIOP), a TCP/IP-based implementation of GIOP. These allow a CORBA-based program from any vendor, on almost any computer, operating system, programming language, and network, to interoperate with a CORBA-based program from the same or another vendor, on almost any other computer, operating system, programming language, and network.

Transaction Processing (TP) monitors provide robust run-time environments for large-scale OLTP applications and offer three important services:

- Process management – includes starting server processes, funneling work to these processes, monitoring the execution, and balancing their workloads.
- Transaction management – the TP monitor guarantees the atomicity, consistency, isolation, and persistency to all programs that run under its protection.
- Client/server communication management – allows clients or services to invoke an application component in a variety of ways.

With TP monitors, the application programmers do not have to concern themselves with issues such as concurrency, failures, broken connections, load balancing, and the synchronization of resources across multiple computer nodes.

The distributed object architecture (e.g., J2EE and CORBA) uses a network communication layer that has three parts: the object server, the skeleton, and the stub. The object server is the business object that resides on the middle tier. The stub resides on the client that initiates the remote invocation. The skeleton resides on the middle tier. The stub and the skeleton make the object server, which lives on the middle tier, act as if it is running locally on the client machine.

#### **4.18.7 Online Transaction Processing**

Online Transactional Processing (OLTP) is characterized by a high volume of transactions, typically organized in a relational data model format. While these systems are structured to provide the response time and concurrency for real-time production systems, OLTP architecture typically does not support analytical requirements that are vital for making corporate strategic decisions necessary for long-term competitiveness. This architectural limitation is addressed by implementing Online Analytical Processing (OLAP) systems along with OLTP systems.

There are two existing OLTP architecture alternatives: (1) a three-tiered client-server, Transaction Processing Monitoring (TPM)-based architecture; or (2) a three-tiered client-server web-based architecture.

Historically, OLTP applications were built using transaction monitors on mainframes and host/terminal-style two-tier architectures. Transaction monitors were required because the operating system was a batch, not an online, system, and the data storage mechanisms did not support the notion of transaction. Modern operating systems, including Novell NetWare Network OS, Microsoft Windows 2000, and various manifestations of UNIX and Linux, directly

support online clients and relational database management systems. Modern high-performance OLTP systems are designed around a conceptual three-tier architecture. In this model, the client-side application and the data all exist as separate logical tiers, tied together with highly scalable middleware. Unlike traditional two-tier architectures, three-tier designs tend to produce lighter-weight clients that are easier to design, manage, and update.

*Required Standards:*

- Systems Engineering Services J2EE standards

#### **4.18.8 Distributed Computing Application Security**

Applications may be required to support integration with a PKI. Another security element is use of a secure server platform for transaction-oriented services for Internet-enabled applications. Features may include a security-hardened operating system hosting a web server that is securely integrated with the trusted operating system (for example, HP Virtual Vault Server and Apache Web Server). The secured server serves as a secure gateway between the web server applications in the external compartment of the trusted operating system and the internal applications or databases. The secured server supports communication with Internet users while only pre-allowed applications in the internal compartment can be executed to communicate with the backend servers.

Other access mechanisms may also be implemented. A secured/hardened proxy server with a filtering mechanism in the DMZ could be placed in front of the web server and serve as a secured gateway. The gateway, along with firewall servers and intrusion detection systems, may provide sufficient layered security protection for certain applications. Another alternative is restricting access to internal servers from servers in a perimeter network/DMZ by only allowing pushes from an internal DCN server to the servers in the perimeter network.

On the application logic level, a J2EE web application server such as WebLogic server from BEA Systems provides role-based declarative security services. The declarative security services provide the ability to administratively declare roles and assign them to application resources. Where and how declarative security is set will determine where security boundaries are drawn for an application. A given role can be assigned to the entire application, an individual component, a particular interface in a component, or to a particular method of an interface.

The data access tier, usually a database server, also has its own security mechanism that allows only an authorized user that has been authenticated to access its information (Note: the user could be an application on the business logic tier).

*Required Standards:*

- [FIPSPUB73](#) Guidelines for Security of Computer Applications, 1980 June 30.

#### 4.18.9 Message Queuing

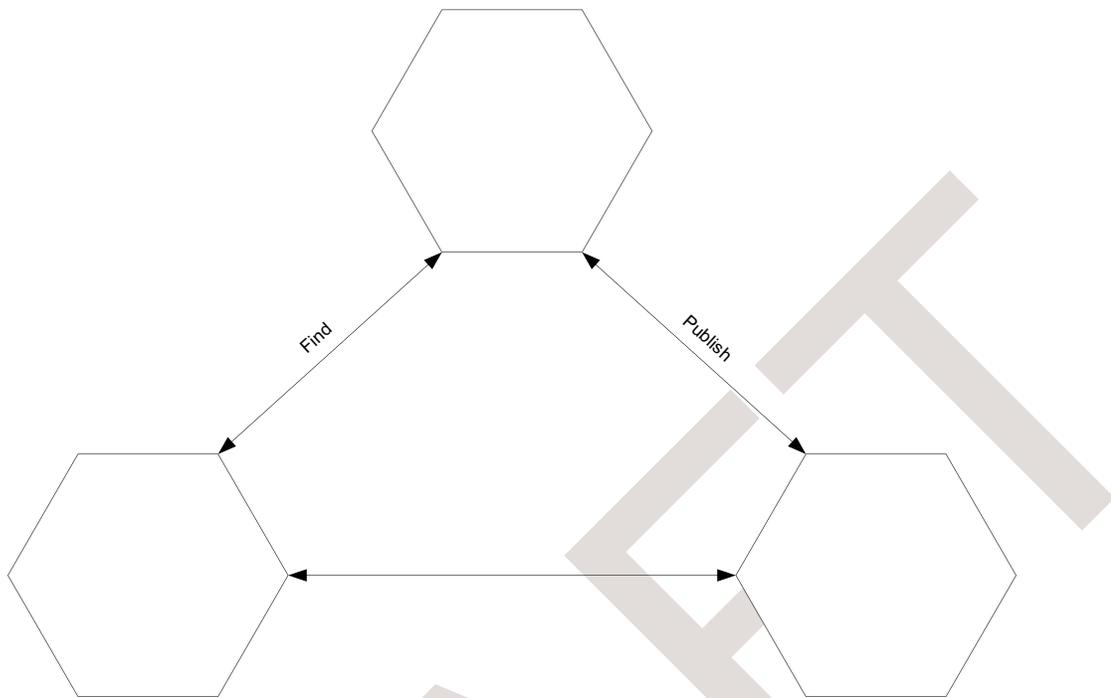
A message queuing service provides a method for applications to process, exchange, and pass data or information from the same operating platform or multiple operating platforms to another. A message queue can be created by one process and used by multiple processes that read and/or write messages to the queue. For example, a server process can read and write messages from and to a message queue created for client processes. In many messaging middleware, message queuing is implemented to provide a buffer for storing messages that have been sent and are waiting to be received. In this message-passing model, the send verb of the API becomes a put-on-queue operation, and the receive verb becomes a get-from-queue operation. In contrast to inter-process communication technologies, message queuing is connectionless (e.g., asynchronous communication). The sender and receiver do not need to be simultaneously available to communicate, nor does the network need to be available directly between the sender and receiver.

#### 4.18.10 Web Services

Web services have gained significant market acceptance recently, and in use by most major enterprises. A web service is a unit of application logic providing data and services to other applications. Applications access web services via ubiquitous web protocols and data formats such as HTTP, XML, and SOAP, without the need to worry about how each web service is implemented. It uses Web Service Description Language (WSDL) to describe a service in a registry and UDDI to facilitate discovery of services. It combines the best aspects of component-based development and the Web. In summary, web services is a platform and implementation independent software component that can be:

- Described using a service description language
- Published to a registry of services
- Discovered through a standard mechanism (at runtime or design time)
- Invoked through a declared API, usually over a network
- Composed with other services

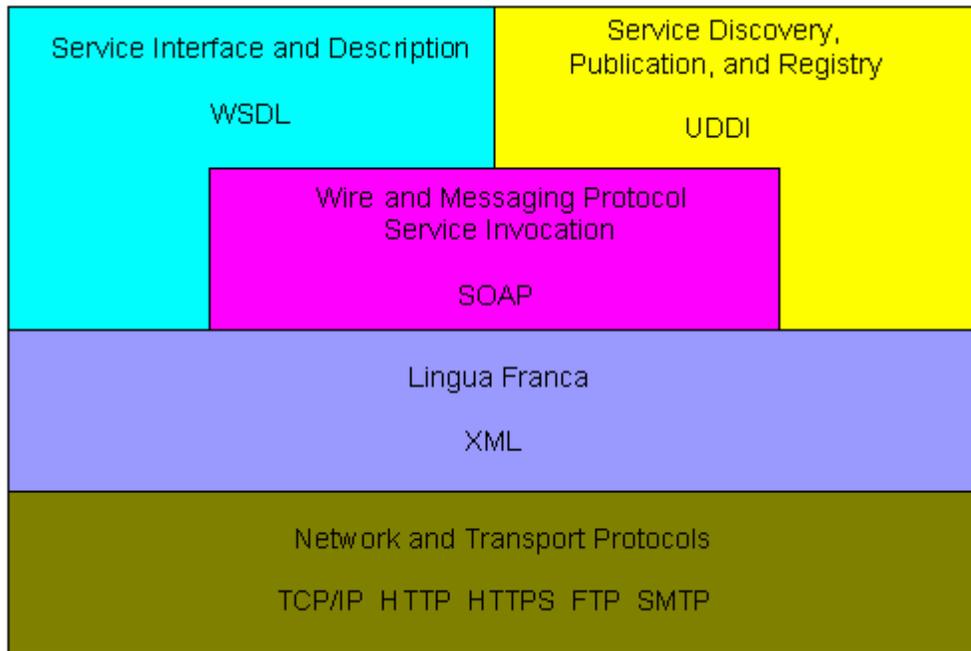
Most web services technologies, when applied to an application integration problem, have a pattern called Service-Oriented Architecture (SOA), as depicted in Figure 4.18-10.



**Figure 4.18-10: Service-Oriented Architecture (SOA)**

A service provider creates a service description, publishes it to one or more service registries, and receives web service invocation messages from one or more service requestors. A service requestor finds a service description from a service registry and uses that description to bind to or invoke the Web service hosted by the specified service provider. A service registry advertises web service descriptions published to it by service providers and allows service requestors to search the collection of service descriptions contained within the service registry.

Figure 4.18-11 from the Gartner Group depicts the technologies forming the Web Services Stack.



**Figure 4.18-11: Web Services Stack**

WSDL provides a standard XML vocabulary and document format that describes web services offered in a service registry. The public UDDI registry – with sites managed by IBM, Microsoft, and Hewlett-Packard and kept in sync with each other – uses WSDL for publishing and dynamic service discovery. Private UDDI registries may or may not support WSDL.

Both WSDL and UDDI show promise in solving inter-organizational integration problems, with WSDL popularity becoming more widespread in recent years.

Development of web services requires strong tool support. Major J2EE development environments such as BEA WebLogic Workshop provide tools for developing and deploying Web services.

While web services or any other XML-based integration technologies provide dynamic binding to services so the integrated partners are decoupled and thus create a flexible and robust partner network, there is overhead in transporting, parsing, and processing XML messages. Internal to an application, the components work with each other tightly and frequently. If XML messages are used as a communication format across layers of an application, the overhead of XML processing can cause degradation to the system performance, especially under heavy load. Systems with tight performance requirements should ensure that this overhead is acceptable. In general, tightly coupled components should communicate through Remote Method Invocation (RMI) or regular local Java method invocation, while loosely coupled components can base their interfaces on standard format such as XML, to hide differences in platforms or languages.

*Required Standard:*

- Emerging technologies/standards includes XML/SOAP/WSDL/UDDI and Java Messaging Services. For further information, refer to  
<http://www.w3.org/TR/>  
<http://www.w3.org/TR/REC-xml>  
<http://www.w3.org/TR/SOAP/>  
<http://www.w3.org/TR/wsdl12>  
<http://java.sun.com/products/jms/vendors.html>  
<http://www.uddi.org>

DRAFT

# Chapter 5 External Environment

## 5.1 Introduction

Figure 5.1-1 depicts the Judiciary External Environment Entity.

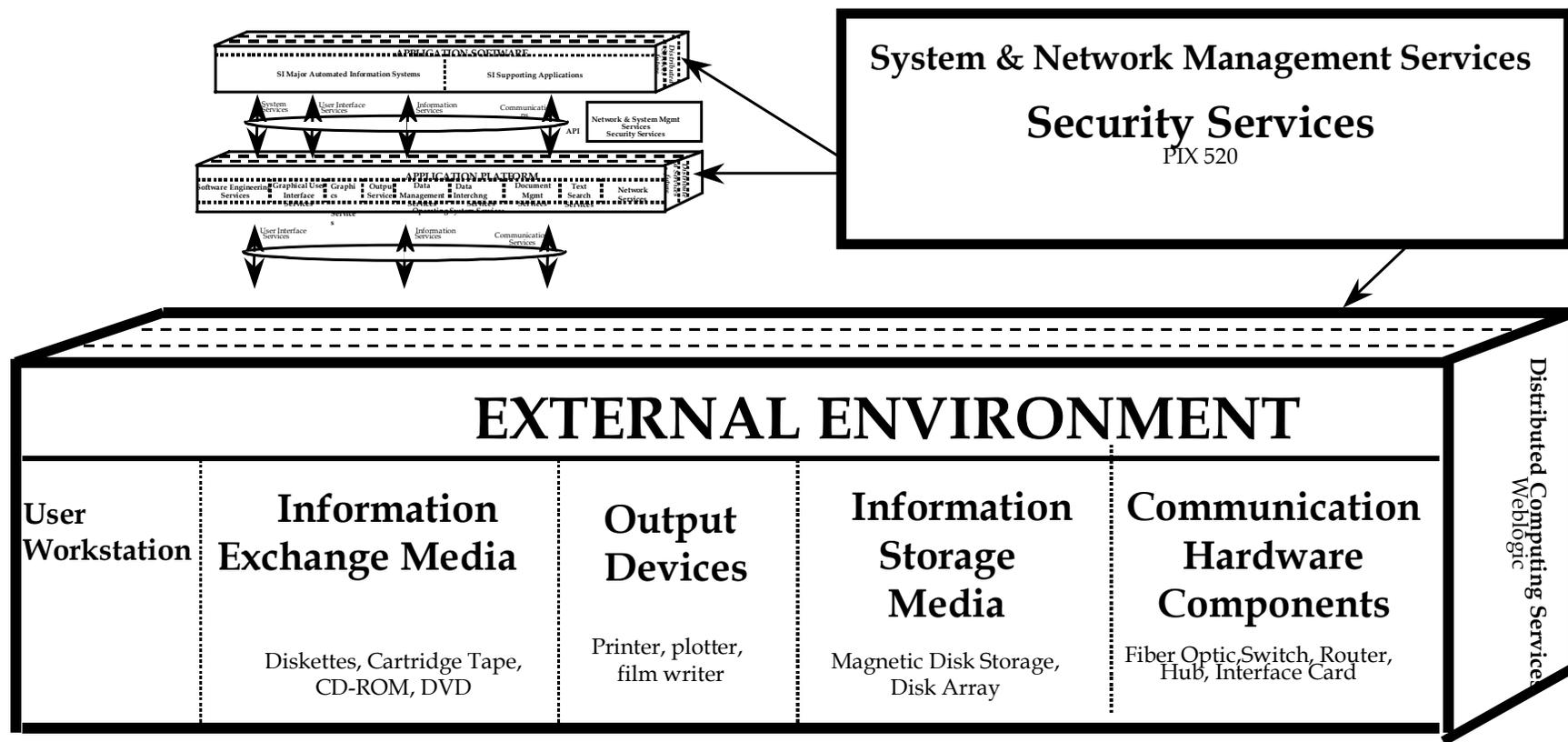


Figure 5.1-1: Judicial External Environment

## 5.2 User Desktop Workstations

Desktop workstations are devices that contain a Central Processing Unit (CPU) and provide a user interface, typically a GUI, as well as personal productivity tools, local data storage, and a method for accessing and manipulating data. (For the associated OS software, please see Section 4.2.)

Desktop workstations are used to support the general office workplace and access to current and planned AISs and IT Infrastructure System Administration functions. The following section provides the preferred workstation hardware configuration for employees of the Judiciary.

**Table 5.2-1: Desktop Workstation Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
The Judiciary has BPAs with Dell, Hewlett-Packard (HP), Gateway, and Micron	Varies by vendor	Desktop workstation	X-86 based workstation	ALL

**Table 5.2-2: Desktop Workstation Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
The Judiciary has BPAs with Dell, HP, Gateway, and Micron		Desktop workstation	X-86 based workstation	ALL

**Table 5.2-3: Desktop Workstation Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Red Hat</a>	Enterprise Linux 4.x	Desktop workstation	X-86 based workstation	ALL

## 5.3 Information Exchange Media

### 5.3.1 Media

Magnetic tapes have been used for nearly 50 years and were the preferred digital storage media for long-term archiving. The three governing factors for the choice of magnetic tapes are cost in terms of bytes per dollar, survivability, and technological evolvability to increased storage density per unit volume. Its major deficiencies result from imposing sequential access thereby limiting scaleable I/O transfer rate increasing in performance as density increases. For over 25 years of electronic computing, 7-track magnetic tapes of 800 bits per inch and 2,400 feet of length were the standard format for the data storage industry. Standards were put into place by most major manufacturers that built tape controllers. The tape media evolved over time to 9-

tracks with 1600 BPI and then to cartridges with more tracks and denser storage. Today a cartridge can hold more than 10 GB compared with the 1960 vintage tapes of less than 1 MB capacity, a 10,000-fold increase. Magnetic disks of varying size, optical disk, CD-ROMs, optical tapes, and other media are now replacing magnetic tape.

Magnetic tape consists of a magnetic particle within a polymer binder that is supported on a backing film. All three of these components—magnetic particle, binder, and backing—are potential sources of failure for a magnetic tape medium. The materials used in the production of diskettes are very similar to that used for magnetic tapes.

The magnetic “pigment” (the terminology is a carry-over from paint and coatings technology) is responsible for storing recorded information magnetically. If there is any change in the magnetic properties of the pigment, data can be irretrievably lost. The magnetic remanence ( $M_r$ ) characterizes the pigment’s ability to retain a magnetic field. The strength of the recorded signal output is related to the magnetic remanence of the pigment. Thus, a decrease in the magnetic remanence of the pigment can result in a low output signal and data loss. The coercivity ( $H_c$ ) characterizes the pigment’s ability to resist demagnetization. Demagnetization can result from an externally applied field, or from self-demagnetization via thermally induced magnetic reversals. A decrease in pigment coercivity makes a magnetic tape more susceptible to demagnetization and signal loss.

The binder is responsible for holding the magnetic particles on the tape and facilitating tape transport. If the binder loses integrity, through softening, embrittlement, or loss of lubrication, the tape may become unplayable and data unretrievable. Polyester polyurethanes are extensively used in tape binder systems. The polyester linkages in these polymers are subject to hydrolysis. Hydrolysis occurs when a polyester group reacts with water to open the polymer linkage, producing an acid and alcohol groups. The produced acid groups further catalyze the hydrolysis reaction. The acid groups can also attack and degrade the magnetic particles. The tape backing, or substrate film, supports the magnetic layer for transportation through the recorder. In general, the tape backing material of choice is an oriented polyethylene terephthalate (PET) film.

The backing is a potential source of tape failure because of dimensional instability of the PET. The dimensions of the backing can change temporarily, as the result of changes in temperature or humidity, or permanently, as the result of polymer creep or relaxation. When a data track is read, it is expected to be at the same location as it was when it was initially laid down during recording. If the read head cannot follow the recorded track on playback, mistracking occurs. Dimensional changes in the backing can alter the length, position, or orientation of data tracks resulting in mistracking and temporary or permanent data loss.

Backing films used for magnetic tape are preferentially oriented in the direction of the tape length. This results in anisotropic, or changed in appearance, film properties. Dimensional changes in the length of the tape will not be proportional to changes in tape width. This applies to dimensional changes induced by changes in temperature/humidity and changes resulting from polymer relaxation. In order to increase the storage capacity of tape cassettes, thinner tape backings are being developed using highly tensilized PET base films. These tensilized films have a greater associated degree of anisotropic film properties and more disproportionate dimensional changes on changes in temperature and humidity.

The magnitude of dimensional backing changes can be reduced through the use of a different backing material. The polyaramid and polyethylene naphthalene (PEN) base films used in some tape products are less subject to dimensional changes as a result of environmental variations than conventional PET.

The susceptibility of the recorded data to loss as a result of dimensional changes in the backing is recording format dependent. Helical scan recording formats can be more susceptible to disproportionate dimensional changes in the backing than longitudinal recordings. Tracks are recorded diagonally on a helical scan tape at small scan angles.

The basic construction of CD-ROM, WORM, and M-O disk media in general consists of a data layer (pits, bumps, or regions of differing physical or magnetic properties) supported on a much thicker polycarbonate or glass substrate, which is read by a laser. A reflective layer is also required for CD-ROM and M-O disks. The data layer/reflective layer is protected with an overcoat. For CD-ROM, the data layer consists of a reflective layer of aluminum with “pits and plateaus” that selectively reflect and scatter the incident laser beam. M-O disks contain a magnetic film that will rotate the polarization of the incident laser beam depending on the local magnetic field recorded on the magnetic “data” layer. In WORM technology, incident laser light is selectively scattered by regions of contrasting optical properties (bumps, pits, or regions of differing physical properties).

Optical discs are generally constructed from polymers and metallics. The polymers are subject to deformation and degradation. Metallic films are subject to corrosion, delamination, and cracking. Metallic alloys are subject to de-alloying. In optical media, there is a data pit (CD-ROM), bump (WORM), or magnetic region (M-O) that is responsible for reflecting/dispersing (CD-ROM, WORM) or rotating the polarization (M-O) of an incident laser beam. Anything that changes the reflectivity, or other optical properties for the data bits can result in a misread. The optical clarity of the substrate is important in those systems where the laser must pass through this layer (CD-ROM, M-O, some WORM). Anything that interferes with the transmission of the beam, such as a scratch, or reduced optical clarity of the substrate, can result in a data error.

CD-ROM technology relies on the difference in reflectivity of “pits” stamped into a polycarbonate substrate and vapor coated with a reflective metallic layer, which is typically aluminum. A common cause of CD-ROM failure is a change in the reflectivity of the aluminum coating as a result of oxidation, corrosion, or delamination. Deterioration of the protective overcoat (acrylic or nitrocellulose lacquer) can make the aluminum layer more susceptible to oxidation and corrosion. Some manufacturers use a silver reflecting layer that is subject to tarnishing by sulfur compounds in the environment and CD-ROM packaging. CD-ROMs can also fail because of deterioration of the polycarbonate substrate. Polycarbonate is subject to crazing, which locally reduces the optical clarity of the substrate. Oils in fingerprints and organic vapors in the environment can contribute to crazing. Scratches in the substrate as a result of mis-handling can also cause disk failures.

Most of the durability problems encountered with M-O disks are associated with degradation of the magnetic layer, which is a metallic film. The layer is subject to corrosion, which has given M-O a poor stability rating in the past. The rare earth-transition metal (RE-TM) alloys are subject to dealloying, which changes the magnetic properties of the data layer. The magnetic

layers on M-O disk can be quite brittle. Subjecting M-O disks to temperature and humidity fluctuations can result in cracking of the magnetic layer.

Manufacturers are providing life expectancy (LE) values for some data storage products. However, there are currently no standard methods for the determination of life expectancies. Without proper qualification of the accelerated test procedures and the life expectancy methods used, values for different vendors and media types cannot easily be compared. Furthermore, LE ratings may be overly optimistic because the test method does not consider many of the significant stress factors found in a “real world” environment.

With moderate care, most magnetic tapes used for digital data storage will last for 10 years. With special storage and handling, digital magnetic tape formats can reliably store information for 30 years or more. Optical disc media can last for several decades. Testing by Imation/3M indicates that their CD-ROM media will last for over 100 years. Research by Kodak shows that their CD-Recordable media is also estimated to last for over 100 years. On the other hand, M-O and phase change disk (PD) media have a life expectancy comparable to magnetic tape of 10–30 years. The actual life expectancy of the media will depend on a number of factors:

- The quality with which the media was manufactured
- The number of times the media is accessed over its lifetime
- The care with which the media is handled
- The storage temperature and humidity
- The cleanliness of the storage environment
- The quality of the recorder used to write to the media

The problem is that digital media, unlike paper, often do not show degradation until it is too late. Occasionally tapes become so brittle that the magnetic coating actually separates from its backing. More often, however, the signs of damage are subtle; routine exposure to everyday magnetic fields will rearrange some of the tape’s magnetized iron particles. When a machine plays the degraded tapes, these alterations make the tapes unreadable, resulting in missing data. In general, media should be handled as follows:

- Store in a cool, dry place.
- Do not leave media sitting around on the desktop, when not in use keep media stored in a clean storage case.
- Avoid flexing or twisting.
- Do not touch media exposed in diskette windows (5-1/4”).
- Do not write directly on the media with a hard tipped pen or pencil.
- Do not expose to magnetic fields (magnetic media).
- If the media is used frequently, maintain a backup copy in the event that the first media becomes unreadable.

Tapes and diskettes both benefit from low storage temperatures and humidities, cleanliness, and proper care and handling. However, compared to tapes, diskettes are much more susceptible to data loss via dirt and mishandling for the following reasons:

- Tapes implement an error correction code (ECC) scheme—if data is missing on one portion of the tape, it may be able to be re-constructed from the redundant information written in the ECC table. Diskettes do *not* employ an ECC scheme. If a data bit gets lost, there is no way to reconstruct it or recover it.
- Diskettes are more susceptible to dirt and mishandling than tapes. Tapes are contained in a durable cartridge with a door that makes it difficult to touch the surface of the tape. 5-1/4” diskettes, however, have exposed media which can easily be contaminated with fingerprints, scratched, or exposed to debris. They are also in flexible containers that can easily be bent. 3-1/2” diskettes are more protected, but debris can still enter the case through the opening near the disk hub.
- Diskettes do not give an indication as to when they are wearing out. A disk could be written one day and be unreadable the next. Some tape systems, on the other hand, will give warning when the media is wearing out as indicated by excessive write errors. This provides an opportunity to replace the old, worn-out tape with a new one before files are irretrievably lost. If a disk is used on a daily basis, a backup of the disk should be made on a regular basis to avoid information loss.
- Debris and wear are the most common causes of information loss from a diskette. If debris gets under the head when the disk is being written, it will not be able to be re-read. If dirt or a fingerprint gets on the diskette it may not be readable. A scratch can remove material that contained a recorded bit of information making the diskette unreadable. If a disk is used every day, the magnetic coating will literally wear out over a period of time. Each time a diskette is read, a small amount of material is worn from the diskette. If enough material is worn from the diskette, the magnetic signal may not be strong enough for the diskette to be read. Furthermore, wear debris particles that are generated can interfere with the reading and writing of diskettes.

### 5.3.2 Tape

Magnetic tape is a common medium for disseminating large volumes of data. For example, an application using this capability might retrieve selected documents from a Judiciary database and copy them to magnetic tape.

With the large size of data collected, backups no longer fit on a single tape. Tape libraries are frequently needed to manage the large sets of tapes needed to provide appropriate backup storage. Smaller libraries can be controlled by simple commands such as “load the next tape in sequence.” Larger tape libraries need software to control and manage the many tapes and, possibly, many tape drives in the library. Since there are no standards for tape libraries it is critical to check with the vendors of both the tape library and the controlling software for compatibility.

#### *Required Standards:*

- ANSI NCITS 311-1998 Information Technology – Magnetic Tape Format for Information Interchange
- ANSI NCITS 312-1998 Information Technology – Magnetic Tape Format for Information Interchange, DLT4 Format

- ANSI NCITS 315-1998 Information Technology – Magnetic Tape Format for Information Interchange, DLT4 Format
- ANSI NCITS 334-2000 Information Technology – Magnetic Tape Format for Information Interchange, DLT3-XT Format
- ANSI NCITS 341-2000 Digital Cartridge Tape Format
- ANSI NCITS 345-2000 Magnetic Tape Cartridge for Information Exchange
- ANSI NCITS 329-2000 DLT5 Format
- Linear Tape-Open (LTO)  
<http://www.lto-technology.com/newsite/index.html>

**Table 5.3-1: Tape Products Used by the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Dell</a>	DLT7000	Backup Device	X-86 based server, MS Windows NT	DOM <sup>1</sup>
<a href="#">Exabyte</a>	Mammoth-2	Backup Device	X-86 based server, Solaris 7	ALL
<a href="#">Exabyte</a>	Mammoth 8900LVD	Backup Device	X-86 based server, Solaris 7	ALL
<a href="#">Exabyte</a>	Eliant 820	Backup Device	X-86 based server, MS Windows 2000	PCT <sup>2</sup>

**Table 5.3-2: Tape Product Preferred Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope
HP	LTO	Backup Device	X-86 based server	ALL

**Table 5.3-3: Tape Product Proposed Products for the Judiciary**

Vendor	Product	Function	Judiciary Platform	Scope

### 5.3.3 CD-ROM Server and Magnetic Optical Disk

Compact Disk-Read Only Memory (CD-ROM) manufacturers and CD-ROM drive software providers use standard specifications for creation of CD-ROM and Compact Disk (CD) recordable media. CD-ROM is one medium of choice for dissemination of custom products. ISO 9660 is the universal standard defining the preferred volume and file structure for all CD-ROM authored disks. It is used across a variety of processing platforms. Virtually all CD-ROM manufacturers and CD-ROM drive software providers use ISO 9660 as the file system for organizing and locating file and directories on CDs; the ISO 9660 standard capacity is .74 GBytes.

*Required Standards:*

<sup>1</sup> DOM: E-Mail server backup medium

<sup>2</sup> PCT: PACTS Report Server

- CDROM Volume File Structure ISO/IEC 9660: 1988

**Table 5.3-4: CD-ROM Products Used by the Judiciary**

Vendor	Product	Model	Function	Scope
Varies	TBD	TBD		

**Table 5.3-5: CD-ROM Preferred Products for the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

### 5.3.4 Digital Versatile Disc Generation Service

Digital Versatile Disc (DVD) services are provided by software used to manage video, audio, linguistic, text, and other resources that are combined into a DVD product. The software may be used to develop a timeline, to associate various files with events on the timeline, create menus and associated program actions, and perform MPEG compression on the video files. After the content is fully “authored”, the DVD service software is used to create a DVD disc image, and testing is executed using simulation.

Required Standards: Emerging standard.

- DVD Version 1.0, 1991. Developed by the DVD Forum, which consists of 17 industry steering committee members and 220 members
- DVD File system based on ISO 13346, subset of Universal Disk Format (UDF)
- ISO 4660, UDF Bridge
- Refer to Data Interchange Standards for DVD, Section 4.10.3

**Table 5.3-6: DVD Products Used by the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

**Table 5.3-7: DVD Preferred Products for the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

### 5.3.5 Scanners

Digitization and creating digital media greatly helps information dissemination and, to some extent, information preservation. Currently information pertaining to collections within the Judiciary is exchanged through direct digital image input, image scanning, and also film.

The Judiciary has a variety of digital imaging and scanning equipment and is expected to purchase similar equipment in the future. For many offices, it is probably most cost-effective to buy multifunction products—which combine copy, print, fax and scan capabilities. Faster processing speeds and print speeds are the key areas of focus. Scan-to-e-mail (scanning and emailing immediately without using computer and other software) is a feature that improves work efficiency.

**Table 5.3-1: Scanning Products Used by the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

**Table 5.3-2: Scanning Preferred Products for the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

## 5.4 Output Devices

### 5.4.1 Displays

Four basic technologies for video display are currently available: direct-view monitors, arrays of monitors (so-called “video walls”), front projection, and rear projection.

Direct-view monitors include typical television sets and computer monitors although they display images with different technical specifications. Modern computer monitors can display images at very high resolution; consumer televisions are more limited.

A video projector is an optical projection device that displays a video image (which can originate from a variety of sources) onto a large screen. This device would be suitable in rooms in which a single large image can be viewed by most of those present. A relatively low level of ambient light may be required for effective use of a front-projection installation.

Video projectors range from small, relatively inexpensive units for standard television signals (usually intended for residential use) to large commercial units that handle multiple signal types varying from standard television signals to high-resolution computer graphics, and which are suitable for images up to 20 feet wide. Like film projectors, video projectors use lenses to focus the image on a screen and can be used either with rear-projection or front-projection screens.

#### 5.4.1.1 Direct View Monitors

With direct-view monitors, the image is viewed directly from the image-producing surface. The most common form of direct-view monitor, the CRT, is used in virtually all televisions and desktop computers. CRTs operate reasonably well in relatively high ambient light. However, they are inherently limited to screens of 35 inches or less (measured diagonally); thus they are limited to relatively small image sizes (typically, 25 inches wide or less).

Another form of direct-view monitor is the Liquid Crystal Display (LCD) panel. This type of screen, which is relatively flat, is commonly used in laptop computers. However, LCD screen

size is limited to even smaller sizes than CRTs, and it is considerably more expensive. LCDs are generally used only where their small size and thinness is essential, such as in laptop computers.

#### **5.4.1.2 Array of Monitors**

Arrays of monitors are becoming popular and are often used for advertising displays. They consist of a grid of CRTs or small self-contained video projection units. One disadvantage is that they have gaps in the image at the “seams” between adjacent units. For computer images or textual displays, the gaps cause loss of information, with details or portions of letters missing.

#### **5.4.1.3 Front Projection**

Front-projection screens, in which the projector is placed in front of the screen on the same side as the audience, work by simply reflecting and diffusing the light from the projector. The disadvantage of front-projection screens is that they reflect the ambient light as efficiently as the light of the image; the room lighting may have to be lowered for usable image contrast. The ability to adjust lighting levels (dimming capability) may be a necessary requirement when front projection is to be used. Also, natural light coming into the room would need to be controlled or blocked out. This type of projector must also be located within a limited distance from the screen to work properly.

#### **5.4.1.4 Rear Projection**

In rear-projection screens, the projector is placed behind the screen on the side opposite the audience. Rear projection works by transmitting and diffusing the light from the projector; ambient light (incident on the front) is not reflected back toward the audience to wash out the image, but is transmitted (in the opposite direction to the image light) into the projection space. Therefore, a rear-projection system can achieve contrast equal to a front-projection system although ambient light levels may be higher. An additional benefit of rear projection is that the equipment is hidden from view, secure from being bumped or tampered with by the audience, and is acoustically isolated from the audience. However, sufficient space must be available behind the screen location to enclose the projector and its associated light path.

### **5.4.2 Printers**

The laser printer works in a similar way to a photocopier, the difference being the light source. With a photocopier a page is scanned with a bright light, while with a laser printer the light source is, not surprisingly, a laser. After that the process is much the same, with the light creating an electrostatic image of the page onto a charged photoreceptor, which in turn attracts toner in the shape of an electrostatic charge.

In inkjet printing, ink is emitted from nozzles as they pass over a variety of possible media, and the operation of an inkjet printer is easy to visualize: liquid ink in various colors being squirted at the paper to build up an image. A print head scans the page in horizontal strips, using a motor assembly to move it from left to right and back, as another motor assembly rolls the paper in vertical steps. A strip of the image is printed, then the paper moves on, ready for the next strip. To speed things up, the print head doesn't print just a single row of pixels in each pass, but a vertical row of pixels at a time.

While lasers and inkjets dominate market share, there are a number of other important print technologies. Solid ink has a significant market presence, being capable of good-quality output on a wide range of media, while thermal wax transfer and dye sublimation play an important role in more specialized fields of printing. Dot matrix technology remains relevant in situations where a fast impact printer is required.

**Table 5.4-1: Printer Products Used by the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

**Table 5.4-2: Printer Preferred Products for the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

## 5.5 Information Storage

Information storage has been around since the earliest computers. Early removable storage was based on paper tape or punch cards. Magnetic tape similar to an audio cassette followed. New removable storage devices can store gigabytes of data on a single disk, cassette, card, or cartridge. There are three major storage technologies, including magnetic storage, optical storage, and solid-state storage.

### 5.5.1 Magnetic Disk Storage

Hard disks are the chief form of storage for computers of all sizes. Though magnetic disk technology is indisputably stable, new innovations are continually squeezing more data into less space, providing faster throughput, and driving costs down. The traditional approach to storage, called server-attached storage, relies on application or network servers running general-purpose operating systems. The disk drives are under the exclusive control of the server, which shares the data on the drives.

Both Network Attached Storage (NAS) and Storage Area Network (SAN) are storage architectures that have gained in popularity since the late 1990s. NAS is defined as a storage system that provides independence to application servers, server hardware architectures, or the server operating system by providing files directly to the user. The NAS model is a mature technology with commodity products available for both small workgroups and enterprise data centers. SAN, on the other hand, represents a state-of-the-art technology that targets organizations with large-scale and complex data storage requirements.

NAS and SAN rely on a number of existing standards related to data networking, including Gigabit Ethernet, TCP/IP, device interface protocols such as Fiber Channel, and reliability standards such as extended data availability and protection attributes (EDAP). The emerging InfiniBand and Storage over IP (SoIP) specifications will likely have future impact on NAS and SAN developments, as well. Network Data Management Protocol (NDMP) addresses the issue of data backups. This initiative defines a standard protocol that storage management applications

can use to back up data in a network of heterogeneous servers. NDMP defines a standard agent that can operate on any file server regardless of hardware platform or operating system.

### 5.5.2 Direct Attached Storage (DAS)

The traditional approach to storage, called server-attached storage, relies on application or network servers running general-purpose operating systems such as Unix (including Solaris, HP-UX, IBM AIX, SGI IRIX, and Linux), Windows NT/2000, and Network Operating Systems such as Novell NetWare. These servers provide access to file systems that can be shared among users while also delivering a variety of other functions such as file services, directory services, distributed printing, mail delivery, web hosting, database transaction processing, and many other network services. The server uses some form of SCSI host adapter or Redundant Array of Independent Disk (RAID) controller that in turn connects to a group or groups of disk drives. The disk drives are under the exclusive control of the server, which shares the data on the drives through protocols such as SMB/CIFS, NFS, or NCP.

The server-attached local disk arrays are RAID storage. RAID offers a cost-effective way to build disk subsystems.

*Required Standard:*

- SNIA (Storage Networking Industry Association) Data Disk Format Technical Working Group, *Common RAID Disk Data Format Specification (R2004)*.  
[www.snia.org/tech\\_activities/ddftwg](http://www.snia.org/tech_activities/ddftwg)

**Table 5.5-1: Direct Attached Storage Products Used by the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

**Table 5.5-2: Direct Attached Storage Preferred Products for the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

### 5.5.3 Network Attached Storage

Network Attached Storage (NAS) devices embody many characteristics of the classic file server, but are stripped of all software features and hardware components except those related to file sharing. They include high-performance network interfaces, typically 100 MB/second Ethernet or Gigabit Ethernet. The hardware architecture is engineered to deliver data from its associated storage devices as efficiently as possible. Relieved of all other duties, a NAS device can be extremely simple to install and configure. Most can be fully functional in a matter of minutes. NAS devices typically do not come with a monitor or keyboard. Users configure and manage these devices remotely through a Web browser, a utility supplied by the vendor, or by direct telnet access. NAS devices make their internal operating system transparent to the end user. Though they run operating systems such as Windows, NetWare, Linux, and proprietary software, they do not require any manual interaction with these environments.

Once connected to the network, NAS devices emulate standard network file servers. They typically appear as exported NFS file systems or as Windows shares through SMB or CIFS. HTTP and FTP access are also standard features. The file systems delivered to the network by a NAS device can either be accessed directly by client computers or can be mounted by application servers. Multiple servers or clients can access a NAS storage volume simultaneously. While NAS devices operate as independent servers, they can leverage the authentication and authorization capabilities of existing servers on the network, eliminating the need to re-create user accounts and access control lists.

**Table 5.5-3: NAS Products Used by the Judiciary**

Vendor	Product	Model	Function	Scope
<a href="#">Dell</a>	NAS Network Storage	PowerVault 51F	Basically a Brocade silkworm 2400 SAN switch 8-port switch for tape backup	
<a href="#">Network Appliance</a>	NAS	NetApp 740	Filer system	
<a href="#">Dell</a>	<a href="#">PowerVault</a>		Disk array storage	
	TBD	TBD		

**Table 5.5-4: NAS Preferred Products for the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

### 5.5.4 Storage Area Networks

Storage Area Networks (SANs) present solutions to many of the problems associated with large-scale data storage. SANs build on the server-attached model through the creation of a separate network of storage devices, independent of the organization’s LAN or communications network. Storage networks can include disk drives, RAID devices, tape libraries, and other storage equipment. Multiple servers, and even client systems, can participate in the storage network to gain access to these devices. The creation of a network of storage devices offers an organization many more options than the traditional approach of connecting storage devices directly to servers.

SANs move data efficiently without adding to the load of the communications network. While LANs use protocols such as Ethernet and TCP/IP, SANs currently rely on fiber channel technologies. In its original and simpler form, Fiber Channel-Arbitrated Loop (FC-AL) connects a limited number of devices in a physical ring topology. More sophisticated SANs use hubs, switches, and routers to create a fiber channel fabric that can include a very large number of devices spanning extensive geographical locations.

The key principle of SAN involves off-loading data transfers from the communications network. In a SAN environment, many data operations can be accomplished without having to traverse the

LAN. Data communications protocols such as Ethernet and IP introduce significant overhead in the transmission, while Fiber Channel technologies dispatch large amounts of data with great efficiency.

The SAN is transparent to network end users. From the perspective of users on the LAN, there are no outward signs to indicate that the network servers rely on a SAN for access to storage devices.

*Required Standards:*

- Reference network services standards related to Gigabit Ethernet, TCP/IP, the Small Computer System Interface (SCSI), Fiber Channel, Serial Storage Architecture (SSA) and Personal Computer Interconnect (PCI).
- Emerging InfiniBand and Storage over IP (SoIP)

**Table 5.5-5: SAN Products Used by the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

**Table 5.5-6: SAN Preferred Products for the Judiciary**

Vendor	Product	Model	Function	Scope
	TBD	TBD		

**5.6 Communications Hardware**

This section covers the physical interconnection and transmission facilities related to accessing services across platforms. This includes data transport, network, data link and physical layers of the network.

**5.6.1 Cables**

Cabling is primarily concerned with the physical layer of the external environment. This includes physical wiring and premise distribution, connection of end-user devices such as LANs, workstations, PCs, terminals and telephones. The physical network transmission medium includes twisted-pair, single mode and multimode fiber optics cables.

*Required Standards:*

- FIPS 159 (also ANSI/EIA/TIA-492AAAA, February 1989 for multimode fiber optics);
- ANSI/EIA/TIA-492BAAA (for single-mode fiber optics)
- ANSI/EIA/TIA 568, Commercial Building Telecommunications for Cabling Standard
- ANSI/EIA/TIA 568B, Commercial Building Telecommunications for Cabling Standard
- ANSI/EIA/TIA 569, Communication Building Standard for Telecommunications Pathway and Spaces (for pathway design)

- ANSI/EIA/TIA 606, Administration Standards for Telecommunications Infrastructure of Commercial Buildings

**Table 5.6-1: Cable Products Used by the Judiciary**

Manufacturer	Product	Model	Function	Scope
	AWG24 Category 5E 4 pair	Copper unshielded twisted pair	Cable	ALL
	AWG24 Category 5E 4 pair	Plenum	Cable	ALL
	AWG24 Category 5 4 pair	Plenum	Cable	ALL
	AWG24 Category 3 4 Pair	Plenum	Cable	ALL
	Micron 8.2/125	Fiber Optics (for singlemode)	Cable	ALL
	Micron 62.5/125	Fiber Optics (for multimode)	Cable	ALL

**Table 5.6-2: Cable Preferred Products for the Judiciary**

Manufacturer	Product	Model	Function	Scope
	AWG24 Category 5E 4 pair	Copper unshielded twisted pair	Cable	ALL
	Micron 8.2/125	Fiber Optics (for singlemode)	Cable	ALL
	Micron 62.5/125	Fiber Optics (for multimode)	Cable	ALL

### 5.6.2 Bridges, Routers, and Switches

A bridge is a network device that is used to send data packets between similar networks. It is a device for forwarding frames between two or more LANs. A router is a network device for interconnecting different types of local area networks and determining the route on which network layer protocol data units should be sent.

**Table 5.6-3: Bridge, Router, and Switch Products Used by the Judiciary**

Vendor	Product	Model	Function	Scope
<a href="#">Cisco</a>	Router	1000 series	Router	ALL
<a href="#">Cisco</a>	Router	2000 series	Router	ALL
<a href="#">Cisco</a>	Router	3000 series	Router	ALL
<a href="#">Cisco</a>	Router	4000 series	Router	ALL
<a href="#">Cisco</a>	Router	5000 series	Router	ALL
<a href="#">Cisco</a>	Router	6000 series	Router	ALL

Vendor	Product	Model	Function	Scope
<a href="#">Cisco</a>	Router	7000 series	Router	ALL

**Table 5.6-4: Bridge, Router, and Switch Preferred Products for the Judiciary**

Vendor	Product	Model	Function	Scope
<a href="#">Cisco</a>	Router	1000 series	Router	ALL
<a href="#">Cisco</a>	Router	2000 series	Router	ALL
<a href="#">Cisco</a>	Router	3000 series	Router	ALL
<a href="#">Cisco</a>	Router	4000 series	Router	ALL
<a href="#">Cisco</a>	Router	5000 series	Router	ALL
<a href="#">Cisco</a>	Router	6000 series	Router	ALL
<a href="#">Cisco</a>	Router	7000 series	R outer	ALL

### 5.7 Satellite Broadcasting/FJTN

Satellite broadcasting equipment enables one site to broadcast an event to multiple sites. Using this capability, video signals are transmitted to a satellite via an uplink. Once the signal reaches the satellite, it is broadcast to sites tuned to receive the broadcast. Satellite broadcasting allows one-way video, in which remote sites can see images (including people, documents, and video) sent from the broadcast studio, but the broadcast studio cannot receive images from the remote sites. Satellite broadcasting in itself does not always allow two-way audio. However, the Federal Judicial Television Network (FJTN) is designed to allow two-way audio in which remote sites can receive audio input from the broadcast studio and the broadcast studio can receive audio input from remote sites equipped with a push-to-talk microphone. The benefit of satellite broadcasting is the ability to reach a multitude of sites simultaneously. Satellite broadcasting is often used for distance learning and information dissemination.

Satellite reception sites are equipped with a satellite antenna and an Integrated Receiver Decoder (IRD). The antenna is a 1.8- meter diameter, fixed-dish antenna, pointing at the GE-3 satellite. The receiver is a PMC SpectrumSaver digital receiver operating in the Ku band. In the TMFJB, a dual function C Band/KU Band, analog antenna is wired into the cable distribution system for the building. A SpectrumSaver IRD is in place. This equipment is capable of accepting vertical or horizontal polarity. Programs received are broadcast over one of three channels. The channels are 38, 39, and 40. In the courts, satellite antennas are being installed with one or more drops within the court building. There is no limit to the number of sites that can receive a broadcast.

Programs presented on the FJTN cover a wide variety of topics such as employee benefits, judicial education, IT and automation, court management and leadership, and administrative and operation programs for judges. The FJTN serves as a means to distribute information and training to large numbers of judicial employees in a timely and cost-effective manner.

**Table 5.7-1: Satellite Broadcasting Products Used by the Judiciary**

<b>Vendor</b>	<b>Product</b>	<b>Model</b>	<b>Function</b>	<b>Scope</b>
	GE-3	Ku band antennas and receivers	Satellite Communications	ALL

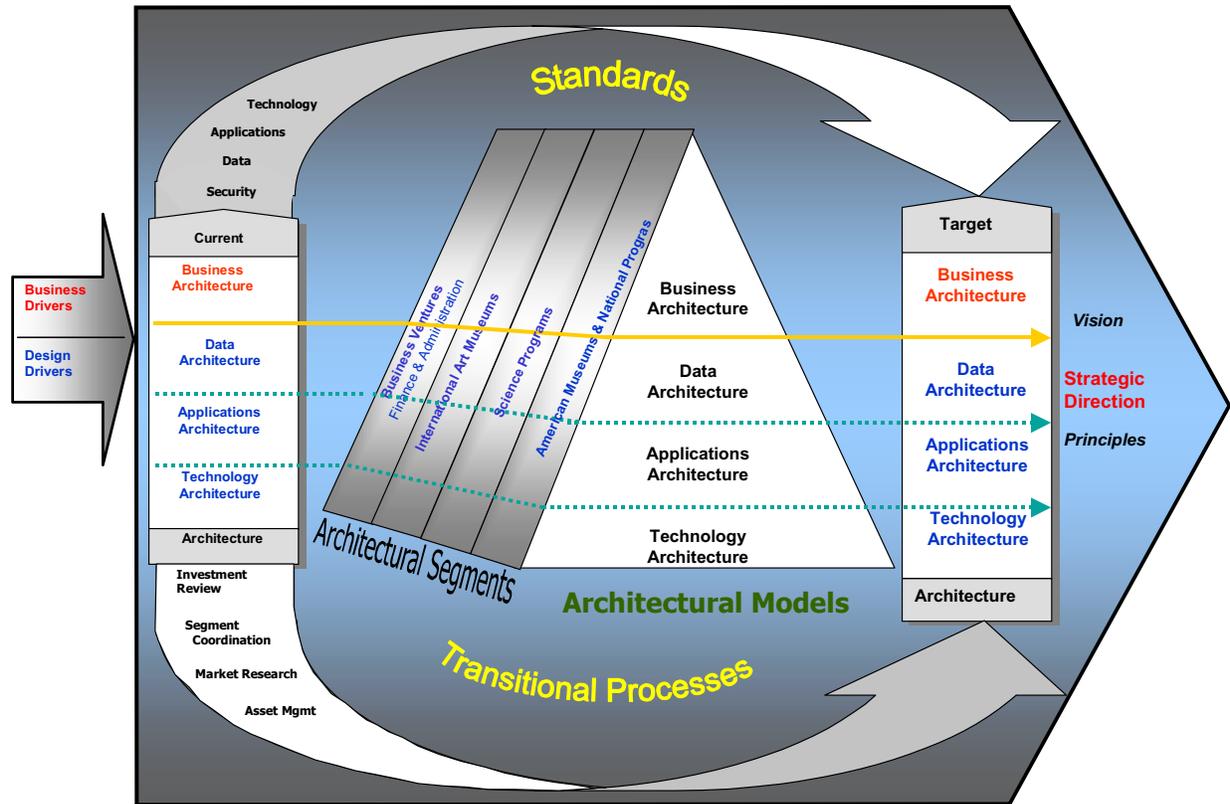
**Table 5.7-2: Satellite Broadcasting Preferred Products for the Judiciary**

<b>Vendor</b>	<b>Product</b>	<b>Model</b>	<b>Function</b>	<b>Scope</b>
	GE-3	Ku band antennas and receivers	Satellite Communications	ALL

# Chapter 6 Judiciary Current and Target Architecture

## 6.1 TRM in the Context of the Federal Enterprise Architecture Framework

The Judiciary has defined an Enterprise Information Technology Architecture (ITA) Strategy that is consistent with the Federal Enterprise Architecture Framework (FEAF)<sup>1</sup>. Figure 6.1-1 depicts the Judiciary concept of the FEAF.



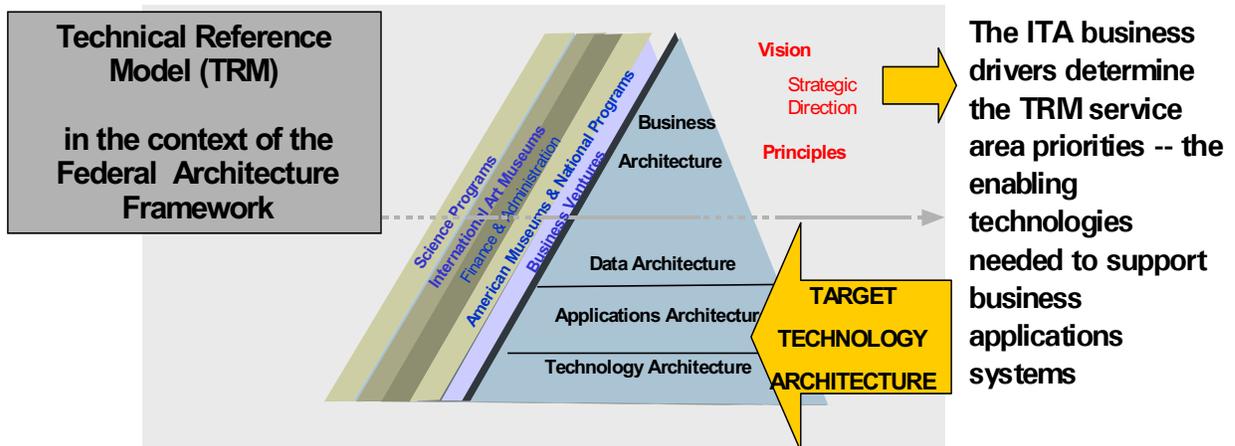
**Figure 6.1-1: Concept of the Federal Enterprise Architecture Framework**

The concept of the FEAF which is graphically represented above is explained in three documents referred to as the Federal Enterprise Architecture 101 – the Trifecta. These are:

- A Practical Guide to Federal Enterprise Architecture, Chief Information Officer Council, Version 1.0, February, 2001
- Federal Enterprise Architecture Framework, Version 1.1, September 1999, CIO Council
- Architecture Alignment and Assessment Guide, October 2000

The TRM has a critical role in the Federal ITA concept of Target Architecture Definition and Gap Analysis. Figure 6.1-2 depicts the Judiciary enterprise target technology architecture strategy.

<sup>1</sup> Reference CIO's Federal Architecture Working Group (FAWG) homepage, <http://www.itpolicy.gsa.gov/mke/archplus/group.htm>



**Target Technology Architecture is governed by defining TRM service area standards & products**

**Figure 6.1-2: Judiciary Enterprise IT Architecture Strategy**

The Judiciary IT Management strategy is consistent with the Federal Architecture Framework Assessment Guide for which the requirements are listed below.

- Requirement 1: Identify Business Process and objectives that will drive IT Architecture.
- Requirement 2: Identify Vision, Objective and IT Principles.
- Requirement 3: Develop and Document the Baseline Architecture.
- Requirement 4: Develop a Technical Reference Model.
- Requirement 5: Develop and Document the Target Architecture.
- Requirement 6: Perform a Gap Analysis Between Current and Target Architecture.
- Requirement 7: Develop a Migration Plan.
- Requirement 8: Achieving Goals of IT Architecture and Electronic Business.

The Technical Reference Model is used to meet Requirements 3, 4, and 5.

## **6.2 Judiciary Profiles of Standards**

The Judiciary current “As-Is” and target “To-Be” architectures are governed by the TRM. All hardware and software components are allocated to a TRM entity. Target Architecture components are defined in terms of Standards and Preferred Products.

### **6.2.1 Open Systems Standards**

The selected standards or specifications include those from national, international and federal standard organizations such as the American National Standards Institute (ANSI), International Organization for Standardization (ISO), Institute of Electrical and Electronic Engineers (IEEE), and International Telecommunications Union (ITU).

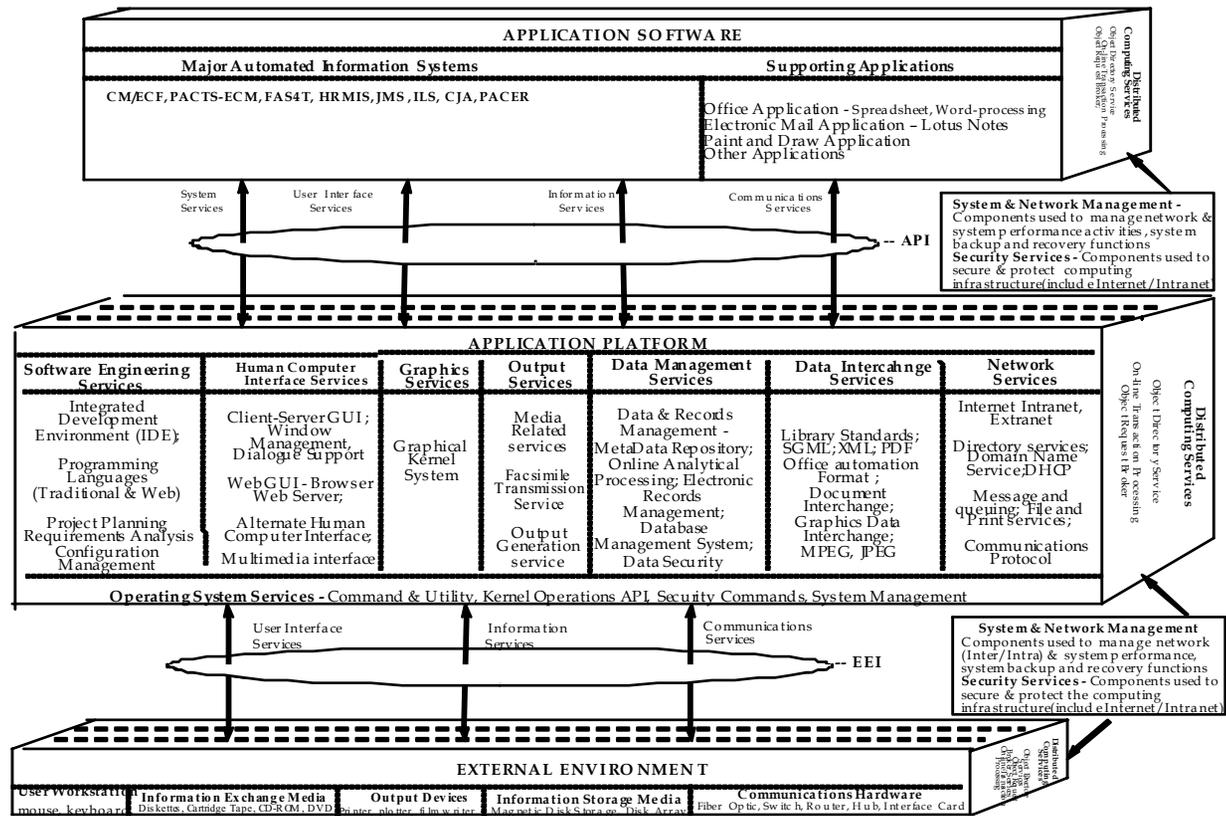
The Judiciary profile of standards is selected based on standards identified by the following:

- Original and updated standards of the *Application Portability Profile (APP)*, Version 3.0, dated February 1996 by National Institute of Standards and Technology (NIST).
- U.S. Machine-Readable Cataloging (MARC) Advisory Committee which includes the American Library Association's (ALA's) Machine-Readable Bibliographic Information (MARBI) committee; U.S. national libraries; the National Library of Canada and the National Library of Australia; the large bibliographic networks such as OCLC and RLIN, library associations such as the Music Library Association and Special Libraries Association; and library system vendors.

Industry, commercial, and government de facto standards are also used.

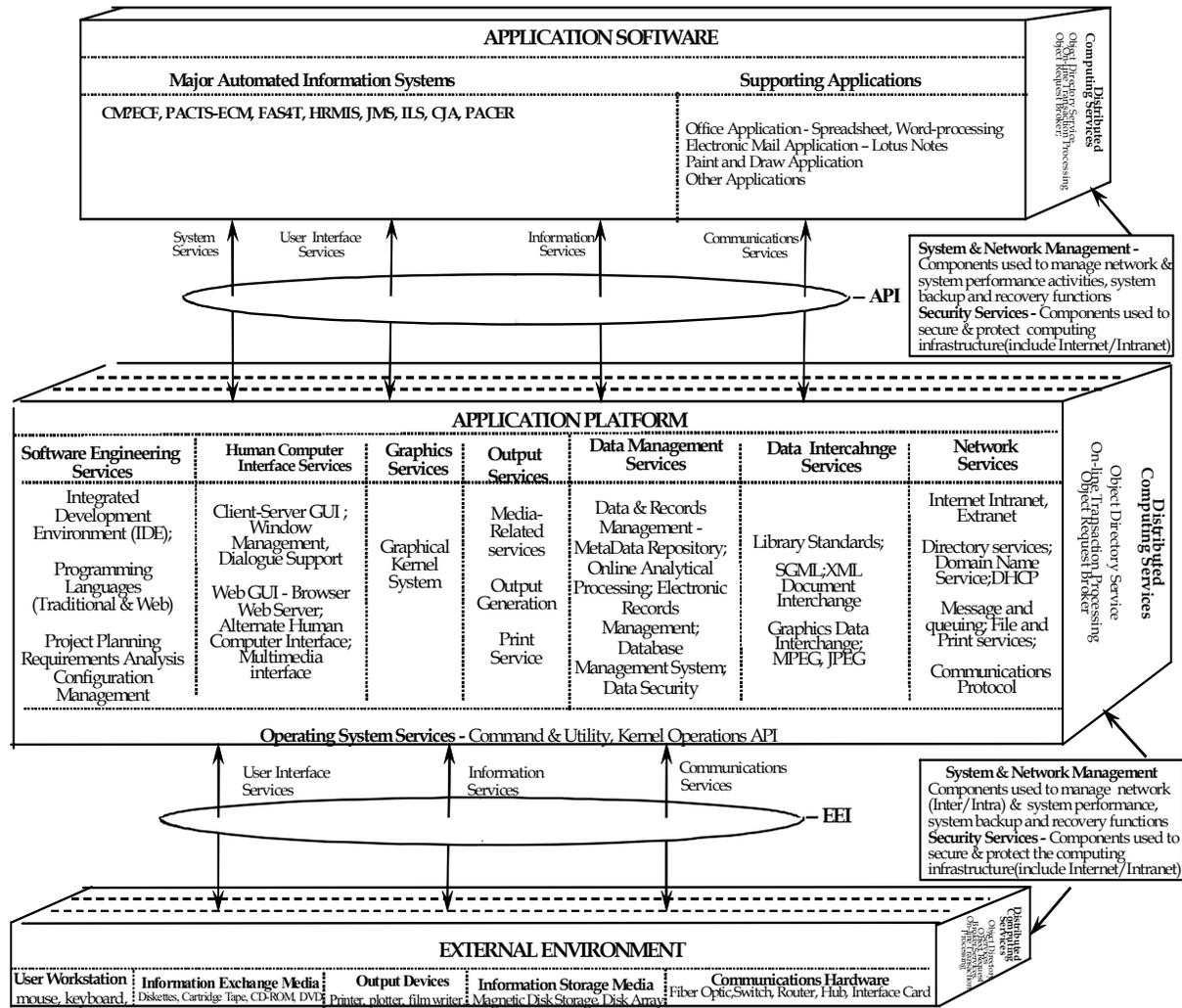
### **6.2.2 Profile of Standards**

Figure 6.2-1 depicts the Judiciary Profile of Standards. Figure 6.2-2 depicts the Judiciary Profile of Preferred Products.



Judiciary Technical Reference Model Detail Level

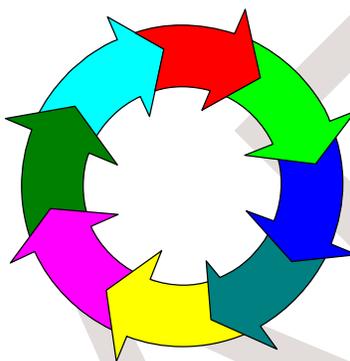
Figure 6.2-1: Judiciary Profile of Standards



### Judiciary Profile of Preferred Products

Figure 6.2-2: Judiciary Profile of Preferred Products

## APPENDICES



## **APPENDIX A ACCESS TO THE TRM**

### **A.1 Access to the TRM**

A copy of the Federal Judiciary's Technical Reference Model can be obtained from the JNet.

### **A.2 Points of Contact**

If you have questions regarding this document please contact:

Richard D. Fennell, Chief Technology Officer

Phone: (202) 502-2730

E-mail: [Rick\\_Fennell@ao.uscourts.gov](mailto:Rick_Fennell@ao.uscourts.gov)

Administrative Office of the U.S. Courts

OIT-CTO, Suite 3-170

One Columbus Circle, NE

Washington, DC 20544

### **A.3 TRM Update Process - Role of TWGs in Recommending a Preferred Product**

Technology Working Groups (TWGs) are subject matter expert (SME) groups focused on specific, emerging, and enabling technologies that the Judiciary needs to apply to work processes (e.g. security, database management, web development, middleware). The goal is to establish *technical* core competency in the specific information technology domain by leveraging resources across the Courts. These activities directly support the broader goals of architecture and engineering interoperability initiatives and enterprise-wide projects. The TWG introduces an internal customer-oriented focus to the existing system architecture staff function, which conducts ongoing investigations of near- and long-term component technologies and performs long-term strategic analysis recommendations for a preferred product for the Judiciary TRM.

## APPENDIX B STANDARDS PROFILE

The Judiciary profile of standards is based on standards identified by the original and updated standards of the *Application Portability Profile* (APP), Version 3.0, dated February 1996 by National Institute of Standards and Technology (NIST), TOGAF Standards Information Base (<http://www.opengroup.org/sib2/>), and industry, commercial, and government de facto standards.

SERVICES	STANDARDS
<p><b>4.3 Operating System Services</b></p>	<p><b>4.3.1 Kernel Operations API</b>            International Standard ISO/IEC 9945-1: 2003, Information technology – Portable Operating System Interface (POSIX)—Part 1: Base Definitions (Incorporates IEEE Std 1003.1-2001/Cor1-2002, Standard for Information Technology—Portable Operating System Interface (POSIX) –Technical Corrigendum 1)  <a href="http://standards.ieee.org/reading/ieee/std_public/description/posix/">http://standards.ieee.org/reading/ieee/std_public/description/posix/</a>  <a href="http://standards.ieee.org/regauth/posix">http://standards.ieee.org/regauth/posix</a>  <a href="http://www.opengroup.org/austin/">http://www.opengroup.org/austin/</a></p> <p><b>4.3.24.3.3 Operating System Commands and Utilities</b>            ISO/IEC 9945-3:2003, Information Technology - Portable Operating System Interface (POSIX) - Part 3: Shell and Utilities  <a href="http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=38791&amp;CSI=35&amp;ICS2=60&amp;ICS3=">http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=38791&amp;CSI=35&amp;ICS2=60&amp;ICS3=</a>  <a href="http://standards.ieee.org/regauth/posix/index.html">http://standards.ieee.org/regauth/posix/index.html</a></p> <p><b>4.3.3 Operating System Management</b>            ISO/IEC 15068-2:1999, Information Technology - Portable Operating System Interface (POSIX) System Administration - Part 2: Software Administration  <a href="http://standards.ieee.org/reading/ieee/std_public/description/posix/">http://standards.ieee.org/reading/ieee/std_public/description/posix/</a>  <a href="http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26362&amp;CSI=35&amp;ICS2=60&amp;ICS3=">http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26362&amp;CSI=35&amp;ICS2=60&amp;ICS3=</a>  <a href="http://ieeexplore.ieee.org/xpl/abs_free.jsp?isNumber=16678&amp;prod=STD&amp;arnumber=770132&amp;arSt=ared=&amp;arAuthor=&amp;arNumber=770132&amp;a_id=770132&amp;count=1">http://ieeexplore.ieee.org/xpl/abs_free.jsp?isNumber=16678&amp;prod=STD&amp;arnumber=770132&amp;arSt=ared=&amp;arAuthor=&amp;arNumber=770132&amp;a_id=770132&amp;count=1</a>  <a href="http://www.opengroup.org/austin">http://www.opengroup.org/austin</a></p> <p><b>4.3.4 Operating System Security</b>            Federal Information Processing Standards Publications (FIPS PUBS)  <a href="http://www.itl.nist.gov/fipspubs/0-toc.htm">http://www.itl.nist.gov/fipspubs/0-toc.htm</a>  <b>FIPSPUB140-2 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, 2001 May 25</b>  <a href="http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf">http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf</a>            FIPS PUB 190 Federal Information Processing Standards Publication 190 1994 September 28 Announcing the Standard for GUIDELINE FOR THE USE OF ADVANCED AUTHENTICATION TECHNOLOGY ALTERNATIVES  <a href="http://www.itl.nist.gov/fipspubs/fip190.htm">http://www.itl.nist.gov/fipspubs/fip190.htm</a>            FIPS PUB 191 Federal Information Processing Standards Publication 191 1994 November 9 Announcing the Standard for GUIDELINE FOR THE ANALYSIS OF LOCAL AREA NETWORK SECURITY  <a href="http://www.itl.nist.gov/fipspubs/fip191.htm">http://www.itl.nist.gov/fipspubs/fip191.htm</a>  <a href="http://www.itl.nist.gov/fipspubs/index.htm">http://www.itl.nist.gov/fipspubs/index.htm</a></p>

SERVICES	STANDARDS
<p><b>4.4 Software Engineering Services</b></p>	<p><b>4.4.2 System Development Methodology</b>  Refer to the Information Resources Management –IRMS 407.0- Applications Software Specifications  <a href="http://jnet.ao/dcn/it/irms407.html">http://jnet.ao/dcn/it/irms407.html</a></p> <p><b>4.4.3 Business Process Re-engineering</b>  International Organization for Standardization (ISO) OMG UML  <a href="http://www.uml.org/">http://www.uml.org/</a>  IEEE/EIA 12207.0-1996/Amd1:2002 Industry Implementation of International Standard ISO/IEC: ISO/IEC12207 Standard for Information Technology Software life cycle processes  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html</a></p> <p><b>4.4.4 Data Modeling</b>  IEEE/EIA 12207.0-1996 Industry Implementation of International Standard ISO/IEC: ISO/IEC12207.0-1996/Amd1:2002 Standard for Information Technology Software life cycle processes  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html</a></p> <p><b>4.4.5 System Development Tools</b>  System Engineering Institute Capability Maturity Model reference  <a href="http://www.sei.cmu.edu/cmm/cmms/transition.html">http://www.sei.cmu.edu/cmm/cmms/transition.html</a>  IEEE Std 1362-1998 (Incorporates IEEE Std 1362a-1998) IEEE Guide for Information Technology – System Definition – Concept of operations (ConOps) Document  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/1362-1998_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/1362-1998_desc.html</a>  IEEE STD 1016-1998 IEEE Guide to Software Design Descriptions  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/1016-1998_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/1016-1998_desc.html</a>  IEEE/EIA 12207.0-1996/Amd1:2002 Industry Implementation of International Standard ISO/IEC: ISO/IEC12207 Standard for Information Technology Software life cycle processes  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html</a>  IEEE Std 2001-1999, IEEE Recommended Practice for Internet Practices – Web Page Engineering – Intranet/Extranet Applications, May 1999  <a href="http://dx.doi.org/10.1041/standard/2001">http://dx.doi.org/10.1041/standard/2001</a>  J2EE standards (Refer to <a href="http://java.sun.com/j2ee/docs.html">http://java.sun.com/j2ee/docs.html</a> and <a href="http://java.sun.com/j2ee/faq.html">http://java.sun.com/j2ee/faq.html</a>)</p>

SERVICES	STANDARDS
<p><b>4.4 Software Engineering Services</b></p>	<p><b>4.4.5.2 Web Application Development</b>  RFC 2616 Hypertext Transfer Protocol  <a href="http://www.rfc-editor.org/rfc/rfc2616.txt">http://www.rfc-editor.org/rfc/rfc2616.txt</a>  <a href="http://www.w3.org/Protocols/">http://www.w3.org/Protocols/</a> for W3C standards on HTTP 1.0 and HTTP 1.1  ANSI NCITS 331.1-1999 Technology - SQLJ - Part 1: SQL Routines Using the Java™ Programming Language  ANSI NCITS 331.2-2000 Information Technology – SQLJ - Part 2: SQL Types using the JAVA™ Programming Language</p> <p><b>4.4.5.3 Web Authoring Tools</b>  Hypertext Markup Language (HTML), subset of SGML, ANSI/ISO 8879:1986<sup>1</sup>  Extensible HyperText Markup Language (XHTML) <a href="http://www.w3.org/TR/xhtml1/">http://www.w3.org/TR/xhtml1/</a><sup>2</sup>  Standard Generalized Markup Language (SGML), ANSI/ISO 8879:1986  Extensible Markup Language (XML) 1.1 (Third Edition), 2004  <i>Standard Overview:</i>  For further information refer to  <a href="http://www.w3.org/TR/html/">http://www.w3.org/TR/html/</a>  <a href="http://www.w3.org/MarkUp/SGML">http://www.w3.org/MarkUp/SGML</a></p> <p><b>4.4.5.4 Traditional Programming Language</b>  ANSI/ISO 9899:1992 - C  FIPS PUB 160, C.  ANSI/ISO/IEC 9899-1999 – Programming Languages – C (revision of ANSI/ISO 9899-1990 (R1997)). <a href="http://www.nssn.org/">http://www.nssn.org/</a>  De facto industry standards used in Visual Basic and Visual C++ by Microsoft Corporation  Java and its associated specifications  The Java language specification. <a href="http://java.sun.com/docs/books/jls/">http://java.sun.com/docs/books/jls/</a>  The Java virtual machine specification. <a href="http://java.sun.com/docs/books/vmspec/">http://java.sun.com/docs/books/vmspec/</a></p> <p><b>4.4.5.5 Web Application Development Language</b>  Java by Sun Microsystems, Inc.  JavaServer Pages™ Specification,  <a href="http://Java.sun.com/products/jsp/download.html">http://Java.sun.com/products/jsp/download.html</a>  Java™ Servlet Specification,  <a href="http://Java.sun.com/products/servlet/download.html">http://Java.sun.com/products/servlet/download.html</a>  Java™ 2 SDK, Enterprise Edition Specification, v 1.4,  <a href="http://java.sun.com/j2ee/1.4/download-sdk.html">http://java.sun.com/j2ee/1.4/download-sdk.html</a>  Enterprise JavaBeans™ Specification,  <a href="http://Java.sun.com/products/ejb/docs.html">http://Java.sun.com/products/ejb/docs.html</a>  Java™ 2Platform, standard Edition specification,  <a href="http://java.sun.com/j2se/">http://java.sun.com/j2se/</a>  Java™ 2 Platform, Micro Edition specification,  <a href="http://java.sun.com/j2me/docs/">http://java.sun.com/j2me/docs/</a>  The Java language specification,  <a href="http://java.sun.com/docs/books/jls/">http://java.sun.com/docs/books/jls/</a>  The Java virtual machine specification,  <a href="http://java.sun.com/docs/books/vmspec/">http://java.sun.com/docs/books/vmspec/</a>  HTML standard 4.01, <a href="http://www.w3.org/TR/html/">HTML Home Page http://www.w3.org/TR/html/</a>  <a href="http://www.w3.org/TR/html/">Extensible Hypertext Markup Language (XHTML) 1.1</a>, W3C's recommendation for the latest version of HTML, <a href="http://www.w3c.org/MarkUp/">http://www.w3c.org/MarkUp/</a> and <a href="http://www.w3c.org/TR/xhtml11">http://www.w3c.org/TR/xhtml11</a></p> <p><b>4.4.6.1 Project Management</b>  <i>IEEE STD 1058-1998 IEEE Standard for Software Project Management Plans</i>  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/1058-1998_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/1058-1998_desc.html</a></p>

SERVICES	STANDARDS
<p><b>4.4 Software Engineering Services</b></p>	<p><b>4.4.6.2 Requirements Management</b>  IEEE STD 830-1998 IEEE Recommended Practice for Software Requirements Specifications  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/830-1998_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/830-1998_desc.html</a>  IEEE STD 1233-1998 IEEE Guide for Developing System Requirements Specifications  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/1233-1998_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/1233-1998_desc.html</a>  System Engineering Institute Capability Maturity Model  <a href="http://www.sei.cmu.edu/cmm/cmms/transition.html">http://www.sei.cmu.edu/cmm/cmms/transition.html</a></p> <p><b>4.4.6.3 Configuration Management</b>  IEEE Std 828-1998, IEEE Standard for Software Configuration Management Plans  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/828-1998_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/828-1998_desc.html</a>  IEEE/EIA 12207.0-1996 Industry Implementation of International Standard ISO/IEC: ISO/IEC12207 Standard for Information Technology Software life cycle processes  <a href="http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html">http://standards.ieee.org/reading/ieee/std_public/description/se/12207_desc.html</a>  The Software Engineering Institute at Carnegie-Mellon University  <a href="http://www.sei.cmu.edu/cmm/cmms/transition.html">http://www.sei.cmu.edu/cmm/cmms/transition.html</a></p>

SERVICES	STANDARDS
<p><b>4.5 Human Computer Interface Services</b></p>	<p><b>4.5.1 Traditional Graphical User Interface</b>  Industry standards used in Visual Interdev, Visual Basic and Visual C++ by Microsoft Corporation  The Windows Interface Guidelines for Software Design</p> <p><b>4.5.2 Web Graphical User Interface</b>  RFC 2616 Hyper Text Transfer Protocol  <a href="http://www.rfc-editor.org/rfc/rfc2616.txt">http://www.rfc-editor.org/rfc/rfc2616.txt</a>  <a href="http://www.w3.org/Protocols/">http://www.w3.org/Protocols/</a> for W3C standards on HTTP 1.0 and HTTP 1.1  HTML standard 4.01, <a href="http://www.w3.org/TR/REC-html40/">HTML Home Page</a> <a href="http://www.w3.org/TR/REC-html40/Extensible%20Hypertext%20Markup%20Language">http://www.w3.org/TR/REC-html40/Extensible Hypertext Markup Language</a> (XHTML) 1.1, W3C's recommendation for the latest version of HTML, <a href="http://www.w3.org/MarkUp/">http://www.w3.org/MarkUp/</a> and <a href="http://www.w3.org/TR/2001/REC-xhtml11-20010531/">http://www.w3.org/TR/2001/REC-xhtml11-20010531/</a>  W3C REC-CSS1-1990111, Cascading Style Sheets, Level 1, W3C Recommendation 17 December 1996, revised 11 January 1999, <a href="http://www.w3.org/TR/1999/REC-CSS1-19990111">http://www.w3.org/TR/1999/REC-CSS1-19990111</a>  W3C REC-CSS1-20040225, Cascading Style Sheets, Level 21, W3C Recommendation  <a href="http://www.w3c.org/TR/CSS21">http://www.w3c.org/TR/CSS21</a></p> <p><b>4.5.2.2 Web Server</b>  HTTP/1.0 and 1.1 (RFC1945 and 2616)  RFC 1945, <a href="http://www.rfc-editor.org/rfc/rfc1945.txt">http://www.rfc-editor.org/rfc/rfc1945.txt</a>  RFC 2616, <a href="http://www.rfc-editor.org/rfc/rfc2616.txt">http://www.rfc-editor.org/rfc/rfc2616.txt</a>  For latest information on W3c standards on HTTP protocol, refer to <a href="http://www.w3.org/Protocols/">http://www.w3.org/Protocols/</a>  DOM (Document Object Model) Level 1, <a href="http://www.w3.org/TR/REC-DOM-Level-1/">http://www.w3.org/TR/REC-DOM-Level-1/</a>  DOM Level 2, <a href="http://www.w3.org/TR/DOM-Level-2/">http://www.w3.org/TR/DOM-Level-2/</a>  W3C HTML home page, <a href="http://www.w3.org/MarkUp/">http://www.w3.org/MarkUp/</a>  HTML 4.01 Specification, W3C Recommendation 24 December 1999, <a href="http://www.w3.org/TR/html4/">http://www.w3.org/TR/html4/</a>  XHTML 1.0, XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition), A Reformulation of HTML 4 in XML 1.0, W3C Recommendation 26 January 2000, revised 1 August 2002 <a href="http://www.w3.org/TR/xhtml1/">http://www.w3.org/TR/xhtml1/</a>  XHTML 1.1, Module-based XHTML, W3C Recommendation 31 May 2001, <a href="http://www.w3.org/TR/xhtml11/">http://www.w3.org/TR/xhtml11/</a>  XML (Extensible Markup Language) 1.0, <a href="http://www.w3.org/XML/">http://www.w3.org/XML/</a>  XML schema, W3C recommendation, May 2001,  <a href="http://www.w3.org/TR/xmlschema-0/">XML Schema Part 0: Primer</a> , <a href="http://www.w3.org/TR/xmlschema-1/">http://www.w3.org/TR/xmlschema-1/</a>  <a href="http://www.w3.org/TR/xmlschema-2/">XML Schema Part 1: Structures</a> <a href="http://www.w3.org/TR/xmlschema-2/">http://www.w3.org/TR/xmlschema-2/</a>  <a href="http://www.w3.org/TR/xmlschema-2/">XML Schema Part 2: Datatypes</a> <a href="http://www.w3.org/TR/xmlschema-2/">http://www.w3.org/TR/xmlschema-2/</a>  RFC 1157, SNMP (Simple Network Management Protocol), <a href="http://www.rfc-editor.org/rfc/rfc1157.txt">http://www.rfc-editor.org/rfc/rfc1157.txt</a>  The Resource Description Framework (RDF) integrates a variety of web-based metadata activities including sitemaps, content ratings, stream channel definitions, search engine data collection (web crawling), digital library collections, and distributed authoring, using XML as interchange syntax. (<a href="http://www.w3.org/RDF/">http://www.w3.org/RDF/</a>).</p> <p><b>4.5.3 Alternate Graphical User Interface</b>  Web Content Accessibility Guidelines 1.0, W3C Organization, <a href="http://www.w3.org/TR/WAI-WEBCONTENT">http://www.w3.org/TR/WAI-WEBCONTENT</a>, 1999.  Section 508 standards, <a href="http://www.section508.gov/final_text.html">http://www.section508.gov/final_text.html</a></p>

SERVICES	STANDARDS
<p><b>4.6 Data Management Services</b></p>	<p><b>4.6.1 Metadata Repository</b>  Online Analytical Processing Service Standards  Database Management System Service Standards  Data Interchange Service Standards  Association Of Systematics Collections Data Model  Federal Geographic Data Standards  Office Of Personnel Management Data Standards</p> <p><b>4.6.3 Online Analytical Processing (OLAP)</b>  ISO/IEC 9075-5/Amd1: 2001 Online Analytical Processing (SQL/OLAP)  ISO/IEC 9075-2/Amd1: 2001 Online Analytical Processing (SQL/OLAP)  ISO/IEC 9075-10:2000 Information technology—Database languages—SQL—Part 10: Object Language Bindings (SQL/OLB)  <a href="http://webstore.ansi.org/ansidocstore/find.asp?">http://webstore.ansi.org/ansidocstore/find.asp?</a>  ISO/IEC 9579-3:1996 Information technology - Open Systems Interconnection - Remote Database Access - Part 3: SQL specialization Protocol Implementation Conformance Statement (PICS) Performance?  ISO/IEC 9579-2:1998 Information technology - Open Systems Interconnection - Remote Database Access - Part 2: SQL Specialization  Microsoft de facto standard Object Link Embedded (OLE) DB for OLAP, OLE 2.0  <a href="http://www.microsoft.com/data/odbc/">http://www.microsoft.com/data/odbc/</a>  JDBC 2.0  <a href="http://java.sun.com/products/jdbc/">http://java.sun.com/products/jdbc/</a>.  Data Interchange Service Standards  JOLAP  <a href="http://jcp.org/en/jsr/detail?id=069">http://jcp.org/en/jsr/detail?id=069</a></p>
<p><b>4.6 Data Management Services</b></p>	<p><b>4.6.6 Document Management</b>  Document Management Alliance Specification (DMA) v1.0  <a href="http://www.infonuovo.com/Dmware/">http://www.infonuovo.com/Dmware/</a>  Open Document Management API (ODMA) v2.0  Extensible Markup Language (XML) Version 1.0 - XML Working Group under the auspices of the World Wide Web Consortium (W3C).  <a href="http://www.w3.org/">http://www.w3.org/</a></p> <p><b>4.6.7 Electronic Records Management</b>  Document Management System Service Standards  Database Management System Service Standards  Data Interchange Service Standards  DoD Records Management Application Standard (DoD 5015.2-STD)  <a href="http://jtc.fhu.disa.mil/recmgt/standards.htm">http://jtc.fhu.disa.mil/recmgt/standards.htm</a></p> <p><b>4.6.8 Web Content Management</b>  Web related Software Engineering Service Standards  Web-related Data Interchange Service Standards  Web-related Network Communications Protocol Standards  RFC 2518 WEBDAV (World Wide Web Distributed Authoring and Versioning) HTTP Extensions for Distributed Authoring and Versioning  <a href="http://www.webdav.org/">http://www.webdav.org/</a> or <a href="http://www.ietf.org/ids.by.wg/webdav.html">http://www.ietf.org/ids.by.wg/webdav.html</a>.  Refer to Web Content Management Standard Section 4.6.8</p> <p><b>4.6.9 Image and Multimedia Management</b>  CompuServe's <a href="#">Graphics Interchange Format (GIF) specification</a>.  Adobe's <a href="#">Tagged Image File Format (TIFF) specification</a>.  Joint Photographic Experts Group Compression Specification - JPEG (also ANSI/ISO IS10918: 1992)</p>

SERVICES	STANDARDS
	<p>World Wide Web's <a href="#">Portable Network Graphics (PNG) specification</a>.  <a href="#">Zsoft's PCX specification</a>.  Macintosh PICT file format.  Adobe's <a href="#">Photoshop specification</a>.  Microsoft's <a href="#">WAV Joint Photographic Experts Group Compression Specification - Standard: Digital Compression and Coding of Continuous-Tone Still Images specification</a>.  ISO MPEG Standards: <a href="#">ISO/IEC-11172</a>, <a href="#">ISO/IEC-13818</a>, <a href="#">ISO/IEC-14496</a>, <a href="#">ISO/IEC JTC1/SC29/WG11</a>, and <a href="#">ISO/IEC JTC1/SC29/WG11/N5231</a>.</p> <p><b>4.6.10 Database Management</b>  FIPS 127-2, Database Language SQL December 3, 1993  <a href="http://www.itl.nist.gov/fipspubs/fip127-2.htm">http://www.itl.nist.gov/fipspubs/fip127-2.htm</a>  ISO/IEC 9075:1992 Information technology – Database languages – SQL  ANSI X3.135-1992 (R1998) Information Systems – Database Language – SQL (includes ANSI X3.168-1989) THE ADOPTION OF ISO/IEC 9075-1, -2, 4 AND -5 WILL RESULT IN THE SUBSEQUENT WITHDRAWAL OF X3.135: 1992  ISO/IEC 9075-9:2001 Information technology – Database languages—SQL—Part 9: Management of External Data (SQL/MED)  ISO/IEC 9075-5:1999 Information technology – Database languages—SQL—Part 5: Host Language Bindings (SQL/Bindings)  ISO/IEC 9075-4:1999 Information technology – Database languages—SQL—Part 4: Persistent Stored Modules (SQL/PSM)  ISO/IEC 9075-3:1999 Information technology – Database languages—SQL—Part 3: Call-Level Interface (SQL/CLI)  ISO/IEC 9075-1:1999 Information technology – Database languages—SQL—Part 1: Framework (SQL/Framework)  ISO/IEC 9075-2:1999 Information technology—Database languages—SQL—Part 2: Foundation (SQL/Foundation)  ISO/IEC 13249-5:2001 Information technology—Database languages – SQL multimedia and application packages—Part 5: Still Image  <a href="http://webstore.ansi.org/ansidocstore/find.asp?">http://webstore.ansi.org/ansidocstore/find.asp?</a></p>

SERVICES	STANDARDS
<p><b>4.6 Data Management Services</b></p>	<p><b>4.6.11 Database Environment</b>  ISO/IEC 9579:1993, Remote Database Access  FIPS 127-2, Database Language SQL December 3, 1993  <a href="http://www.itl.nist.gov/fipspubs/fip127-2.htm">http://www.itl.nist.gov/fipspubs/fip127-2.htm</a>  ISO/IEC 9075:1992 Information technology - Database languages – SQL  ANSI X3.135-1992 (R1998) Information Systems – Database Language – SQL  (includes ANSI X3.168-1989) THE ADOPTION OF ISO/IEC 9075-1, -2, 4 AND -5  WILL RESULT IN THE SUBSEQUENT WITHDRAWAL OF X3.135: 1992  ISO/IEC 9579-3:1996 Information technology - Open Systems  Interconnection - Remote Database Access - Part 3: SQL Specialization  Protocol Implementation Conformance Statement (PICS) proforma  ISO/IEC 9579-2:1998 Information technology - Open Systems Interconnection -  Remote Database Access - Part 2: SQL Specialization  ANSI NCITS 331.1-1999 Technology - SQLJ - Part 1: SQL Routines Using the  JavaTM Programming Language  ANCITS 331.2-2000 Information Technology - SQLJ - Part 2: SQL Types using the  JAVATM Programming Language  <a href="http://webstore.ansi.org/ansidocstore/find.asp?">http://webstore.ansi.org/ansidocstore/find.asp?</a>  JDBC 2.0  <a href="http://java.sun.com/products/jdbc/">http://java.sun.com/products/jdbc/</a>.  ODBC Microsoft de facto standard, <a href="http://www.microsoft.com/data/odbc/">http://www.microsoft.com/data/odbc/</a></p> <p><b>4.6.12 Data Management Security</b>  NIST Special Publication 800-8  ISO/IEC 9579:2000 Information technology – Remote database access for SQL with  security enhancement  <a href="http://webstore.ansi.org/ansidocstore/find.asp?">http://webstore.ansi.org/ansidocstore/find.asp?</a></p>

SERVICES	STANDARDS
<p><b>4.7 Data Interchange Services</b></p>	<p><b>4.7.1 Financial and Human Resources Technical Standards</b>  The <i>Joint Financial Management Improvement Program</i> (JFMIP)  <a href="http://www.jfmip.gov/jfmip/">http://www.jfmip.gov/jfmip/</a>  The <i>Federal Accounting Standards Advisory Board</i> (FASAB) <a href="http://www.fasab.gov/">http://www.fasab.gov/</a>  The <i>Central Personnel Data File</i> (CPDF) <a href="http://www.opm.gov/feddata/">http://www.opm.gov/feddata/</a> and  <a href="http://www.opm.gov/feddata/guidance.htm">http://www.opm.gov/feddata/guidance.htm</a></p> <p><b>4.7.2 Library Interchange Standards</b>  U.S. MARC (Machine-Readable Cataloging) Advisory Committee standards  MARC (Machine-Readable Cataloging) <a href="http://www.loc.gov/marc/">http://www.loc.gov/marc/</a>  <a href="http://lcweb.loc.gov/marc/status.html">http://lcweb.loc.gov/marc/status.html</a>  ANSI Z39.2, Information Interchange Format BIBLIOGRAPHIC INFORMATION INTERCHANGE  ANSI X3.4, Code for Information Interchange (ASCII) CODED CHARACTER SETS-7-BIT AMERICAN NATIONAL STANDARD  ANSI Z39.47, Extended Latin Alphabet Coded Character Set for Bibliographic Use (ANSEL)  <a href="#">ISO 2709, Format for Information Exchange</a>  <a href="#">NISO Z39.71, Holdings Statements for Bibliographic Items</a>  <a href="#">Z39.50</a> Information Retrieval Standard (copy to search – proposals for searching between information systems; used with SIRIS)  UNICODE Unicode is based on ISO 10646, Universal Character Set (UCS)  ALA (American Library Association) Character set  ANSI Z39.56, Serial Item and Contribution Identifier (SICI)  -CODABAR Barcode standards  -Z39.19, Guidelines for Construction, Format, and Management of Monolingual Thesauri (pertains to AFA thesaurus)  Dublin Core: this is ANSI Z39.85, Dublin Core Metadata Element Set Dublin Core Metadata Element Set, Version 1.1: Reference Description, 1999-07-02,  <a href="http://dublincore.org/documents/dces/">http://dublincore.org/documents/dces/</a>  NISO 2001-07-02, (the NISO version of the Dublin Core element set)  ISO/IEC 11179 [ISO11179] standard for the description</p>

SERVICES	STANDARDS
<p><b>4.7 Data Interchange Services</b></p>	<p><b>4.7.3 Unicode Standard</b>  The Unicode Consortium Unicode incorporates ISO/IEC 6937 and ISO/IEC 8859 families of standards  SGML standard ISO/IEC 8879  Bibliographic standards ISO 5426  ANSI Z39.64, KS C 5601, JIS X 0209, JIS X 0212, GB 2312, and CNS 11643  Industry code pages and character sets from Adobe, Apple, Fujitsu, Hewlett-Packard, IBM, Lotus, Microsoft, NEC, and Xerox  References section of The Unicode Standard, Version 3.0,  <a href="http://www.unicode.org/unicode/standard/standard.html">http://www.unicode.org/unicode/standard/standard.html</a>  Unicode Character Set (UCS) - ISO/IEC 10646-1:2000 Information Technology— Universal Multiple-Octet Coded Character Set (UCS)--Part 1: Architecture and Basic Multilingual Plane, which is also known as the Universal Character Set (UCS).</p> <p><b>4.7.4 Markup Languages</b></p> <p><b>4.7.4.1 Standard Generalized Markup Language (SGML)</b>  ANSI/ISO 8879:1986,  <a href="http://www.w3.org/MarkUp/SGML/">http://www.w3.org/MarkUp/SGML/</a></p> <p><b>4.7.4.2 Extensible Markup Language (XML)</b>  1.0, <a href="http://www.w3c.org/XML/">http://www.w3c.org/XML/</a>  XML schema, W3C recommendation, May 2001,  XML Schema Part 0: Primer , <a href="http://www.w3c.org/TR/xmlschema-0/">http://www.w3c.org/TR/xmlschema-0/</a>  XML Schema Part 1: Structures <a href="http://www.w3c.org/TR/xmlschema-1/">http://www.w3c.org/TR/xmlschema-1/</a>  XML Schema Part 2: Datatypes <a href="http://www.w3c.org/TR/xmlschema-2/">http://www.w3c.org/TR/xmlschema-2/</a>  For further information, refer to <a href="http://www.w3c.org/XML/">http://www.w3c.org/XML/</a></p> <p><b>4.7.4.3 HyperText Markup Language (HTML)</b>  Document Object Model (DOM) Level 2 HTML Specification  Version 1.0, W3C Recommendation 09 January 2003  <a href="http://www.w3c.org/TR/DOM-Level-2/">http://www.w3c.org/TR/DOM-Level-2/</a>  W3C HTML home page, <a href="http://www.w3c.org/MarkUp/">http://www.w3c.org/MarkUp/</a>  HTML 4.01 Specification, W3C Recommendation 24 December 1999,  <a href="http://www.w3c.org/TR/html4/">http://www.w3c.org/TR/html4/</a></p> <p><b>4.7.4.4 Extensible HyperText Markup Language (XHTML)</b>  XHTML 1.0, XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition), A Reformulation of HTML 4 in XML 1.0, W3C Recommendation 26 January 2000, revised 1 August 2002 <a href="http://www.w3c.org/TR/xhtml1/">http://www.w3c.org/TR/xhtml1/</a>  XHTML 1.1, Module-based XHTML, W3C Recommendation 31 May 2001,  <a href="http://www.w3c.org/TR/xhtml11/">http://www.w3c.org/TR/xhtml11/</a></p> <p><b>4.7.4.5 Cascading Style Sheets</b>  Cascading Style Sheets, level 2, CSS2 Specification, W3C Recommendation 12-May-1998, <a href="http://www.w3c.org/TR/REC-CSS2/">http://www.w3c.org/TR/REC-CSS2/</a></p> <p><b>4.7.4.6 Extensible Stylesheet Language (XSL)</b>  The Extensible Stylesheet Language (XSL), <a href="http://www.w3c.org/Style/XSL/">http://www.w3c.org/Style/XSL/</a>  Mathematical Markup Language (MathML) Version 2.0, W3C Recommendation 21 February 2001</p> <p><b>4.7.5 Portable Document Format (PDF)</b>  Portable Document Format Reference Manual, forth edition, version 1.4, 2003 by Adobe Systems Incorporated - Industry Standard  <a href="http://partners.adobe.com/asn/acrobat/docs/File_Format_Specifications/PDFReference.pdf">http://partners.adobe.com/asn/acrobat/docs/File_Format_Specifications/PDFReference.pdf</a></p>

SERVICES	STANDARDS
<p><b>4.7 Data Interchange Services</b></p>	<p><b>4.7.7 Office Automation File Formats</b> RTF standard – Rich Text Format specification version 1.7</p> <p><b>4.7.8 Calendar Date and Ordinal Date Interchange Format</b> American National Standard ANSI X3.30-1997: Representation of Date for Information Interchange (revision of ANSI X3.30-1985 (R1991)). <a href="http://web.ansi.org/public/std_info.html">http://web.ansi.org/public/std_info.html</a> FIPS PUB 4-2, "Representation of Calendar Date for Information Interchange", November 15, 1998. ISO 8601:2000, <i>Data Elements and Interchange Formats - Information Interchange – Representation of Dates and Times</i> <a href="http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26780&amp;ICS1=1&amp;ICS2=140&amp;ICS3=30">http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=26780&amp;ICS1=1&amp;ICS2=140&amp;ICS3=30</a> <a href="http://www.itl.nist.gov/fibspubs/fips4-2.html">http://www.itl.nist.gov/fibspubs/fips4-2.html</a></p> <p><b>4.7.9 Vector Graphics</b> Scaleable Vector Graphics (SVG) 1.1 Specification; W3C Recommendation 14 January 2003. <a href="http://www.w3.org/TR/SVG11/">http://www.w3.org/TR/SVG11/</a> ANSI/8632.1-4:1192[1994], ANSI.ISO 8632/Amd.1: 1994, ANSI/ISO 8632:1992/Adm.2: 1995, MIL-D-28003A. FIPS 128-2</p> <p><b>4.7.10 Raster Image Interchange</b> ISO/IEC 12064-1:1995 International Standardized Profile; and Consultative Committee for International Telephony and Telegraphy (CCITT) Group 4 Raster Image Standard</p> <p><b>4.7.11 Tagged Image File Format</b> TIFF (Tag Image File Format) Revision 6.0 <a href="http://partners.adobe.com/asn/developer/PDFS/TN/TIFF6.pdf">http://partners.adobe.com/asn/developer/PDFS/TN/TIFF6.pdf</a></p> <p><b>4.7.12 Joint Photographic Experts Group (JPEG)</b> Joint Photographic Experts Group Compression Specification - JPEG (also ANSI/ISO IS10918-1 (ITU-T T.81)) Standard: Digital Compression and Coding of Continuous-Tone Still Images <a href="http://www.jpeg.org/public/jpeghomepage.htm">http://www.jpeg.org/public/jpeghomepage.htm</a></p> <p><b>4.7.13 Motion Picture Experts Group (MPEG)</b> ISO Information technology – Coding of audio-visual objects, <a href="#">ISO/IEC-11172</a>, <a href="#">ISO/IEC-13818</a> and <a href="#">ISO/IEC-14496</a>, <a href="#">ISO/IEC JTC1/SC29/WG11</a>, and <a href="#">ISO/IEC JTC1/SC29/WG11/N5231</a>. ISO MPEG Standards: <a href="#">ISO/IEC-11172</a>, <a href="#">ISO/IEC-13818</a>, <a href="#">ISO/IEC-14496</a>, <a href="#">ISO/IEC JTC1/SC29/WG11</a>, and <a href="#">ISO/IEC JTC1/SC29/WG11/N5231</a>.</p> <p><b>4.7.14 Electronic Data Interchange</b> The PAN American (EDI for administration, Commerce, and Transport) EDIFACT Board or United Nations Economic Commission for Europe for the EDIFACT family of EDI standards (The U.S. input to EDIFACT development is through the Pan American EDIFACT Board, one of the five EDIFACT boards.) The American National Standards Institute (ANSI) and the Data Interchange Standards Association (DISA) for the X12 family of EDI standards (this is for the U.S. implementation of EDI) <a href="http://www.ietf.org/html.charters/ediint-charter.html">http://www.ietf.org/html.charters/ediint-charter.html</a></p> <p><b>4.7.15 Computer-Aided Design (CAD) Data</b> Computer-Aided Design/Computer-aided Manufacturing (CAD/CAM) ANSI Y14.26-1989; and IGES 5.2 (US PRO/IPO-100)</p>

SERVICES	STANDARDS
<p><b>4.8 Graphics Services</b></p>	<p><b>4.8 Graphics Services</b>  O/IEC 8651-4:1991 – Information processing systems – Computer graphics— Graphical Kernel System (GKS) language bindings  ANSI INCITS 124-1985 (R2002)- Graphical Kernel System (GKS) Functional Description (includes ANSI X3.124.1-1985) (formerly ANSI Standard X3.124-1985 (R1996))  ISO 7942:1985 -- Information technology—Computer graphics and image processing—Graphical Kernel System (GKS)  INCITS/ISO/IEC 8632-1-1999- Computer Graphics – Metafile for the Storage and Transfer of Picture Description Information- Part 1 : Functional Specification  INCITS/ISO/IEC 8632-3-1999- Computer Graphics – Metafile for the Storage and Transfer of Picture Description Information- Part 3 : Binary Encoding  INCITS/ISO/IEC 8632-4-1999- Computer Graphics – Metafile for the Storage and Transfer of Picture Description Information- Part 4 : Clear Text Encoding  [Note: there does not appear to be a Part 2 with the CGM standard]</p>
<p><b>4.10 Output Services</b></p>	<p><b>4.10.2 Compact Disk-Read Only (CD-ROM) Generation Service</b>  CD-ROM Volume/File Structure ISO/IEC ISO 9660:1988  Refer to Electronic Data Interchange Standards Section 4.7.14</p> <p><b>4.10.3 Digital Versatile Disc (DVD) Generation Service</b>  DVD Version 1.0, 1991. Developed by the DVD Forum, which consists of 17 industry steering committee members and 220 members.  DVD File system based on ISO 13346, subset of Universal Disk Format (UDF) ISO 4660, UDF Bridge  Refer to Electronic Data Interchange Services Standards Section 4.7.14</p> <p><b>4.10.4 Digital Video and Film Generation Service</b>  ISO/IEC 13818-2: 2000 Information Technology – generic coding of moving pictures and associated audio information; video; parts.</p> <p><b>4.10.5 Magnetic Tape Generation Service</b>  ANSI NCITS 311-1998 Information Technology – Magnetic Tape Format for Information Interchange  ANSI NCITS 312-1998 Information Technology – Magnetic Tape Format for Information Interchange, DLT4 Format  ANSI NCITS 315-1998 Information Technology – Magnetic Tape Format for Information Interchange, DLT4 Format  ANSI NCITS 334-2000 Information Technology – Magnetic Tape Format for Information Interchange, DLT3-XT Format  ANSI NCITS 341-2000 Digital Cartridge Tape Format  ANSI NCITS 345-2000 Magnetic Tape Cartridge for Information exchange  ANSI NCITS 329-2000 DLT5 Format  Linear Tape-Open (LTO)  <a href="http://www.lto-technology.com/newsite/index.html">http://www.lto-technology.com/newsite/index.html</a></p> <p><b>4.10.7 Print Service</b>  ISO DPA 10175 - Document Printing Applications  POSIX 1387.4 - Printing Interfaces  CCITT Group 4 Raster Image</p>

SERVICES	STANDARDS
<p><b>4.11 Network Services</b></p>	<p><b>4.11.4 File and Print Service</b>            POSIX 1003.1 standard            POSIX 1003.8 Transparent File access specification            RFC 959 File Transfer Protocol (FTP)  <a href="http://www.w3.org/Protocols/RelevantProtocols.html">http://www.w3.org/Protocols/RelevantProtocols.html</a>  <a href="http://www.rfc-editor.org/rfcxx00.html#STDbyRFC">http://www.rfc-editor.org/rfcxx00.html#STDbyRFC</a>            ISO 8571 File Transfer, Access and Management, Information Systems—Open Systems Interconnection—File Transfer, Access and Management.  <a href="http://www.iso.ch/iso/en/Standards_SearchStandardsQueryForm">http://www.iso.ch/iso/en/Standards_SearchStandardsQueryForm</a></p> <p><b>4.11.5 Directory and Naming Services</b>            Lightweight Directory Access Protocol (LDAP)            LDAP v2, v3. LDAPv3, is an update developed in the IETF (Internet Engineering Task Force), which address the limitations found during deployment of the previous version of LDAP, RFC 1779  <a href="http://www.ietf.org/rfc.html">http://www.ietf.org/rfc.html</a> or  <a href="http://www.ietf.org/iesg/1rfc_index.txt">http://www.ietf.org/iesg/1rfc_index.txt</a>.</p> <p><b>4.11.6 Domain Name Service (DNS)</b>            RFC 1034, Domain Names—Concepts and Facilities            RFC 1035, Domain Names—Implementation and Specification            RFC 1996, addendum to RFC 1035            RFC 2308 March 1998, update RFC 1034 and RFC 1035  <a href="http://www.rfc-editor.org/rfcxx00.html#STDbyRFC">http://www.rfc-editor.org/rfcxx00.html#STDbyRFC</a></p> <p><b>4.11.7 Electronic Mail, Message Services</b>            RFC 2045 MIME - Multipurpose Internet Mail Extension  <a href="#">RFC 2633</a>, RFC 2632, RFC 2634 S/MIME Secure/Multipurpose Internet Mail Extensions            RFC2060 IMAP Internet Message Access Protocol - Version 4rev1            RFC821 SMTP Simple Mail Transfer Protocol</p> <p><b>4.11.8 Time Services</b>            RFC 1305, NTPV3 – Network Time Protocol (Version 3) Specification, Implementation</p>
<p><b>4.12 Video- conferencing</b></p>	<p><b>4.12 Video-conferencing</b>            H.320 – Standard for addressing ISDN Videoconferencing  <a href="http://www.imtc.org/h320.htm">http://www.imtc.org/h320.htm</a>            H.323 – Standard for addressing Video (Audiovisual) communication on Local Area Network. <a href="http://www.imtc.org/h323.htm">http://www.imtc.org/h323.htm</a>            H.324 – Standard for addressing High Quality Video and Audio Compression over POTS modem connections. <a href="http://www.imtc.org/h324.htm">http://www.imtc.org/h324.htm</a></p>
<p><b>4.13 Virtual LAN (VLAN)</b></p>	<p><b>4.13 Virtual LAN (VLAN)</b>            IEEE 802.1Q</p>
<p><b>4.14 Voice Over IP (VoIP)</b></p>	<p><b>4.14 Voice Over IP (VoIP)</b>            H 225 - Call signaling protocols and media stream packetization for packet-based multimedia communication systems.  <a href="http://www.itu.int/rec/recommendation.asp?type=folders&amp;lang=e&amp;parent=T-REC-H.225.0">http://www.itu.int/rec/recommendation.asp?type=folders&amp;lang=e&amp;parent=T-REC-H.225.0</a>            H.323 v2/v3 ITU Standards, <a href="http://www.imtc.org/h323.htm">http://www.imtc.org/h323.htm</a></p>

**4.15  
Communication  
Protocols**

**4.15.2 Transmission Control Protocol/Internet Protocol (TCP/IP)**

RFC791 (IP)  
RFC793 (TCP)  
RFC768 (UDP)  
For further information on RFCs, refer to  
<http://www.rfc-editor.org/rfcxx00.html#STDbRFC> and search by RFC#.

**4.15.3 Ethernet**

IEEE 802.3 (ISO 8802)  
IEEE 802.3, 2000 Edition (also ISO/IEC 8802-3:2000) are available at  
<http://standards.ieee.org/catalog/IEEE802.3.html> or refer to  
[http://www.iso.ch/iso/en/Standards\\_Search.StandardsQueryForm](http://www.iso.ch/iso/en/Standards_Search.StandardsQueryForm) and search for ISO  
#8802

**4.15.3.1 Gigabit Ethernet**

Gigabit Ethernet – IEEE 802.3z or IEEE 802.3ab.  
<http://standards.ieee.org/catalog/IEEE802.3.html>, <http://www.gigabit-ethernet.org>, or  
<http://www.10gea.org/Tech-whitepapers.htm>

**4.15.4 Wireless LAN (WLAN)**

Wireless LAN – IEEE 802.11b  
IEEE 802.11a  
IEEE 802.11g  
[http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/airo\\_ov.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao340ap/prodlit/airo_ov.htm)

**4.15.6 Asynchronous Transfer Mode (ATM)**

Open System Interconnection (OSI)  
Specifications and standards are those adopted by the ATM Forum and the Internet  
Engineering Task Force (IETF).  
Standard for Multi-Protocol over ATM (MPOA) is deployed on the network.  
Standard for Multi-Protocol over ATM version 1.1  
<ftp://ftp.atmforum.com/pub/approved-specs/af-mpoa-0114.000.pdf>  
Standard for silence suppression, voice compression, and variable-bit-rate (VBR)  
service will emerge.

**4.15.6.1 LAN Emulation (LANE)**

The ATM Forum's LANE version 1.0  
<ftp://ftp.atmforum.com/pub/approved-specs/af-lane-0021.000.pdf>  
IEEE 802.3 Ethernet

**4.15.6.3 Multi-Protocol Over ATM (MPOA)**

Open System Interconnection (OSI)  
Multi-Protocol Over ATM Version 1.1  
<ftp://ftp.atmforum.com/pub/approved-specs/af-mpoa-0114.000.pdf>

<b>4.15 Communication Protocols</b>	<p><b>4.15.7 Dynamic Host Configuration Protocol (DHCP)</b> RFC 2131, Dynamic Host Configuration Protocol—an Internet Proposed Standard Protocol by Dynamic Host Configuration Working Group of the Internet Engineering Task Force (IETF)</p> <p><b>4.15.8 Hypertext Transfer Protocol (HTTP)</b> HTTP—RFC 2774, Hypertext Transfer Protocol HTTP/1.1, February 2000, by the Internet Engineering Task Force/W3C (IETF/W3C) HTTP development group <a href="http://www.w3.org/Protocols/">http://www.w3.org/Protocols/</a></p> <p><b>4.15.9 Uniform Resource Locator (URL)</b> URL—RFC 2700, August 2000 - Internet Engineering Task Force (IETF) Network Working Group. <a href="http://www.ietf.org/rfc/rfc2700.txt?number=2700">http://www.ietf.org/rfc/rfc2700.txt?number=2700</a></p> <p><b>4.15.10 Multipurpose Internet Mail Extensions (MIME)</b> RFC 2045: MIME Part One: Format of Internet Message Bodies RFC 2046: MIME Part Two: Media Types RFC 2047: MIME Part Three: Message Header Extensions for Non-ASCII Text RFC 2048: MIME Part Four: Registration Procedures RFC 2049: MIME Part Five: Conformance Criteria and Examples <a href="http://www.oac.uci.edu/indiv/ehood/MIME/MIME.html">http://www.oac.uci.edu/indiv/ehood/MIME/MIME.html</a>, <a href="http://www.rfc-editor.org/rfc.html">http://www.rfc-editor.org/rfc.html</a> or <a href="http://www.rfc-editor.org/rfcxx00.html#STDbyRFC">http://www.rfc-editor.org/rfcxx00.html#STDbyRFC</a> for further information</p>
---	--

**4.16  
Security  
Services**

**4.16.1.1 Secure Firewall**

[COMMON CRITERIA for Information Technology Security Evaluation \(CC\) VERSION 2.1 / ISO IS 15408 FIPS 140-1](#)

**4.16.1.2 Intrusion Detection**

The Intrusion Detection Working Group (IDWG) has created a standards-based method whereby IDS products and components can interoperate. The two end products of the IDWG are the IDMEF (Intrusion Detection Message Exchange Format) and the IDXP (Intrusion Detection Exchange Protocol). These specify the data format and exchange procedures, respectively. For further information, please refer to <http://www.ietf.org/html.charters/idwg-charter.html>.

**4.16.3.1 Password Usage**

FIPS 112, Password Usage

**4.16.4.1.2 Public-Key or Asymmetric Cryptography**

RSA is ANSI Standard X9.44

**4.16.4.1.3 Data Encryption Standard (DES)**

FIPS 46-3 Data Encryption Standard (DES) replaces FIPS 46-2 to recognize Triple DES.

ANSI X9.52 (Triple DES)

ANSI X3.92-1981

FIPS 81, DES Modes of Operation also ANSI3.106

FIPS 197 Advanced Encryption Standard (AES)

**4.16.4.3 Virtual Private Network (VPN)**

FIPS 140-1, Security Requirements for Cryptographic Modules.

**4.16.4.5 Public-Key Infrastructure**

FIPS 140-1, Security Requirements for Cryptographic Modules.

The Internet Engineering Task Force (IETF) RFC 2144 - CAST, a symmetric key algorithm used within Entrust Product.

**4.16.4.5.1 Digital Signature Standard (DSS)**

FIPS 186, Digital Signature Standard (DSS) (also Draft ANSI X9.30-199x Part 1; and ISO/IEC JTC1/SC27/WG2, Project 1.27.08 Digital Signature with Appendix)

[FIPSPUB186-2](#) DIGITAL SIGNATURE STANDARD (DSS), 2000 January 27

**4.16.4.5.2 Digital Certificate Authentication (x.509)**

International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) (formerly called Consultative Committee on International Telephony and Telegraphy (CCITT) X.509, Certificate Authentication

<p><b>4.16 Security Services</b></p>	<p><b>4.16.4.5.4 Secure Hash Standard (SHS)</b>  <a href="http://www.itl.nist.gov/fipspubs/fip180-2.htm">http://www.itl.nist.gov/fipspubs/fip180-2.htm</a>- FIPS 180-2, SECURE HASH STANDARD (SHS), 2000 August, for SHA-1 algorithm. SHA-1 is a technical revision of SHA (FIPS 180)</p> <p><b>4.16.4.6.1 Transport Layer Security</b>          TLS Protocol Version 1.0, RFC 2246 (based on The Secure Sockets Layer (SSL version 3.0) - Internet Engineering Task Force (IETF)).</p> <p><b>4.16.4.6.3 Secure Multipurpose Internet Mail Extensions (S/MIME)</b>          Public Key Cryptography Standard (PKCS) #7 - Cryptographic Message Syntax Standard. This standard was created in 1991 by a consortium of computer industry vendors including Apple, Digital, Lotus, MIT, RSA, and SUN.          RFC 2015: MIME Security with Pretty Good Privacy (PGP).  <a href="#">IP Authentication using Keyed MD5 (RFC 1828)</a>  <a href="#">The ESP DES-CBC Transform (RFC 1829)</a>  <a href="#">HMAC: Keyed-Hashing for Message Authentication (RFC 2104)</a>  <a href="#">HMAC-MD5 IP Authentication with Replay Prevention (RFC 2085)</a>  <a href="#">Security Architecture for the Internet Protocol (RFC 2401)</a>  <a href="#">The NULL Encryption Algorithm and Its Use With IPsec (RFC 2410)</a>  <a href="#">IP Security Document Roadmap (RFC 2411)</a>  <a href="#">IP Authentication Header (RFC 2402)</a></p> <p><b>4.16.4.6.4 Message-Digest Algorithms</b>          RFC 1319: The MD2 Message-Digest Algorithm.          RFC 1321: The MD5 Message-Digest Algorithm.</p>
<p><b>4.17 System and Network Management Services</b></p>	<p><b>4.17.1 Network Systems Administration</b>          Reference Operating Systems Services Standards          Reference Network Services Standards</p> <p><b>4.17.2 Help Desk Administration</b>          Reference Operating Systems Services Standards          Reference Network Services Standards</p> <p><b>4.17.3 Communication Network Management</b>          Reference Network Services Standards          SNMP (Simple Network Management Protocol)</p> <p><b>4.17.4 Server Management</b>          SNMP (Simple Network Management Protocol)</p>
<p><b>4.18 Distributed Computing Services</b></p>	<p><b>4.18.7 Online Transaction Processing (OLTP)</b>          Systems Engineering Services J2EE standards</p> <p><b>4.18.10 Web Services</b>          Emerging technologies/standards includes XML/SOAP/WSDL/UDDI and Java Messaging Services. For further information, refer to  <a href="http://www.w3.org/TR/">http://www.w3.org/TR/</a>  <a href="http://www.w3.org/TR/REC-xml">http://www.w3.org/TR/REC-xml</a>  <a href="http://www.w3.org/TR/SOAP/">http://www.w3.org/TR/SOAP/</a>  <a href="http://www.w3.org/TR/wsdl12">http://www.w3.org/TR/wsdl12</a>  <a href="http://java.sun.com/products/jms/vendors.html">http://java.sun.com/products/jms/vendors.html</a></p>

<p><b>5.3 Information Exchange Media</b></p>	<p><b>5.3.2 Tape</b> ANSI NCITS 311-1998 Information Technology – Magnetic Tape Format for Information Interchange ANSI NCITS 312-1998 Information Technology – Magnetic Tape Format for Information Interchange, DLT4 Format ANSI NCITS 315-1998 Information Technology – Magnetic Tape Format for Information Interchange, DLT4 Format ANSI NCITS 334-2000 Information Technology – Magnetic Tape Format for Information Interchange, DLT3-XT Format ANSI NCITS 341-2000 Digital Cartridge Tape Format ANSI NCITS 345-2000 Magnetic Tape Cartridge for Information exchange ANSI NCITS 329-2000 DLT5 Format Linear Tape-Open (LTO) <a href="http://www.lto-technology.com/newsite/index.html">http://www.lto-technology.com/newsite/index.html</a></p> <p><b>5.3.3 CD-ROM Server and Magnetic Optical Disk</b> CDROM Volume File Structure ISO/IEC 9660: 1988</p> <p><b>5.3.4 Digital Versatile Disk (DVD) Generation Service</b> Emerging standard DVD Version 1.0, 1991. Developed by the DVD Forum, which consists of 17 industry steering committee members and 220 members. DVD File system based on ISO 13346, subset of Universal Disk Format (UDF) ISO 4660, UDF Bridge Refer to Data Interchange Standard Section 4.10.3</p>
<p><b>5.5 Information Storage</b></p>	<p><b>5.5.2 Server Attached Local Disk Array</b> RAID</p> <p><b>5.5.4 Storage Area Networks (SAN)</b> Reference network services standards related to Gigabit Ethernet, TCP/IP, the Small Computer System Interface (SCSI), Fiber Channel, Serial Storage Architecture (SSA) and Personal Computer Interconnect (PCI). Emerging InfiniBand and Storage over IP (SoIP)</p>
<p><b>5.6 Communica- tion Hardware</b></p>	<p><b>5.6.1 Cables</b> FIPS 159 (also ANSI/EIA/TIA-492AAAA, February 1989 for multimode fiber optics); ANSI/EIA/TIA-492BAAA (for single-mode fiber optics) ANSI/EIA/TIA 568, Commercial Building Telecommunications for Cabling Standard ANSI/EIA/TIA 568B, Commercial Building Telecommunications for Cabling Standard ANSI/EIA/TIA 569, Communication Building Standard for Telecommunications Pathway and Spaces (for pathway design) ANSI/EIA/TIA 606, Administration Standards for Telecommunications Infrastructure of Commercial Buildings</p>

## APPENDIX C JUDICIARY PROFILE OF PREFERRED PRODUCTS

The following set of tables represents the preferred products identified in the preceding chapters and sections. In some cases products are “to be defined”, or there may be a large set of preferred products listed because additional analysis needs to be performed.

### C.1 CHAPTER 4- APPLICATION PLATFORM ENTITY

#### 4.3 Operating System Services

##### 4.3.1 Kernel Operations API

Vendor	Operating System	Function	Judiciary Platform	Scope
<a href="#">Red Hat</a>	Linux	Enterprise servers	X-86 based server	ALL
<a href="#">Microsoft</a>	Windows 2000, XP	Desktop workstation	X-86 based workstation	ALL
<a href="#">Microsoft</a>	Windows 2000, XP	Notebook	X-86 based notebook	ALL
<a href="#">Hewlett Packard</a>	Windows CE	Handheld	HP iPAQ	PCT <sup>1</sup>
<a href="#">Palm</a>	Palm OS	Handheld	Palm	

<sup>1</sup> PCT: Mobile Data Access

##### 4.3.2 Operating System Commands and Utilities

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Red Hat</a>	Linux Advanced Server	Operating System Utilities	X-86 based servers	ALL
	SSH	Encrypted terminal connections	X-86 based servers, Linux	ALL

##### 4.3.3 Operating System Management

Vendor	Product	Function	Judiciary Platform	Scope
OS Vendor	Management Utilities bundled with the OS	OS Management Utilities	X-86 servers, Linux	ALL
<a href="#">American Power Conversion</a>	Powerchute	Interface to UPS	X-86 servers, Linux	ALL

##### 4.3.4 Operating System Security

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Tripwire</a>	Tripwire Software	Monitor changes in critical files	X-86 based server, Linux	ALL

## 4.4 Software Engineering Services

### 4.4.3 Business Process Re-engineering

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Business modeling solution		ALL

### 4.4.4 Data Modeling

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data modeling solution		

#### 4.4.5.1 Primary System Development Tools

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Crystal Decisions</a>	Crystal Reports 8.0, 9.0	Report Writer	X-86 based workstation, MS Windows 95, 98, ME, NT, 2000, XP	
<a href="#">IBM</a>	Lotus Notes Designer	Notes Application Development	X-86 based workstation, MS Windows 95, 98, ME, NT, 2000, XP	AO

#### 4.4.5.2 Web Application Development

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Adobe</a>	Acrobat 5.0	PDF generator	X-86 based workstation, Linux, Microsoft Windows 2000, XP	ALL
<a href="#">Peoplesoft</a>	Peopletools 8.4	Integrated Development Environment to develop Web applications for commercial Peoplesoft	X-86 based workstation, Linux, Microsoft Windows 2000, XP	HRM <sup>1</sup>

<sup>1</sup> HRM: Used by Human Resources Management, not entire judiciary

#### 4.4.5.3 Web Authoring Tools

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.4.5.4 Traditional Programming Language

Vendor	Programming Language	Scope
Open Source	Perl5	ALL
Open Source and Proprietary	C / C++	ALL
<a href="#">Sun Microsystems</a>	<a href="#">Java (J2SE 1.3.1, J2EE 1.2, J2ME)</a>	ALL
<a href="#">IBM</a>	VS Fortran	AO
<a href="#">IBM</a>	OS/VS COBOL	AO
<a href="#">IBM</a>	VS COBOL	AO

#### 4.4.5.5 Web Application Development Language

Vendor	Programming Language	Scope
<a href="#">Sun Microsystems</a>	<a href="#">Java - Java2 J2SE 1.3, or later;</a> <sup>3</sup>	ALL
Vendor independent	HTML / XML	ALL
	Javascript	ALL
Open source	Perl5	ALL

#### 4.4.5.6 Web Application Development Environment (IDE)

Vendor	Product	Function	Judiciary deployment Platform	Scope
TBD				

#### 4.4.6.1 Project Management (PM)

Vendor	Product	Function	Platform	Scope
<a href="#">Microsoft</a>	Project 2002	Project Management	X-86 based workstation, Microsoft Windows 2000, XP	ALL

#### 4.4.6.2 Requirements Management (RM)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.4.6.3 Configuration Management (CM)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

### 4.5 Human Computer Interface Services

#### 4.5.1 Traditional Graphical User Interface

Vendor	Product	Function	Judiciary Platform	Scope
			X-86 based workstation	

##### 4.5.2.1 Web Browser

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Microsoft</a>	Internet Explorer 6.x, 128 bit encryption	Web browser provides client interconnection services to access Judiciary or public networks.	X-86 based workstation, MS Windows 2000, XP	
<a href="#">Netscape</a>	Netscape Communicator 7.x, 128 bit encryption	Web browser provides client interconnection services to access Judiciary or public networks.	X-86 based workstation, Linux, MS Windows 2000, XP; X-86 based servers, Linux	
	Mozilla	Web browser provides client interconnection services to access Judiciary or public networks.	X-86 based workstation, MS Windows 95, 98, ME, NT, 2000, XP X-86 based server	

##### 4.5.2.2 Web Server

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Apache Software foundation</a>	Apache 2x	Intra/internet Web Server A reference implementation of the HTTP protocol	X-86 based servers, Linux	ALL
<a href="#">BEA Systems</a>	WebLogic	Web application server (Used bundled with commercial applications)	X-86 based servers, Linux	FAS <sup>1</sup>

<sup>1</sup> FAS: FAS4T waiver

#### 4.5.3 Alternate User Interface

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.5.4 Multimedia Interface

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.5.5 Terminal Emulation

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

### 4.6 Data Management Services

#### 4.6.1 Metadata Repository

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.2 Metadirectory Services

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.3.1 Online Analytical Processing (OLAP) Servers

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.3.2 Desktop and Online Analytical Processing (OLAP / DOLAP)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.4 Data Extraction, Transformation, and Load (ETL) Tools

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.5 Search Services

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.6 Document Management

Vendor	Product	Function	Judiciary deployment Platform	Scope
<a href="#">WorkDynamics Technologies</a>	ccmMercury	Imaging and Workflow		AO
<a href="#">EiStream Technologies</a> <sup>1</sup>	OPEN/Image			AO
<a href="#">IBM</a>	Lotus Domino.Doc	Workflow	X-86 based server, Linux	AO
<a href="#">TMSSequoia</a>	Prizm Plug-in	Browser Plug-In to Handle Images	X-86 based workstation, MS Windows 2000, XP	AO
<a href="#">TMSSequoia</a>	GrayFix	Improves grayscale images		AO
<b>Pegasus Software</b>	ImageN V 3.0			AO

<sup>1</sup>Note: EiStream took over Eastman Software; Vredenburg was a distributor of Eastman Software products.

#### 4.6.7 Electronic Records Management (ERM)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.8 Web Content Management (WCM)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.9 Image and Multimedia Management Systems

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.10 Database Management Systems (DBMS)

Vendor	Product	Function	Judiciary deployment Platform	Scope
<a href="#">IBM</a>	Informix 9	Multi-user Relational Database	X-86 based server, Linux	
<a href="#">Microsoft</a>	Access XP	For less than 10 concurrent users on a server Database Use Only, Including Minimal development work	X-86 based workstation, MS Windows 2000, XP	
	MySQL	Multi-user Relational Database	X-86 based server, Linux	

#### 4.6.11 Database Environments

Vendor	Product		Judiciary Platform	Scope
<a href="#">IBM</a>	Informix 9 <sup>1</sup>		X-86 based servers, Linux	

<sup>1</sup> Informix will continue to be the Judiciary Database for the life of the present contract. A waive may be considered if third party products that are required by a project will not support Informix. The third party products must either be on the TRM Preferred/To Be list or will have to get waivers themselves.

#### 4.6.12 Data Management Security

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

### 4.7 Data Interchange Services

#### 4.7.1 Financial and Human Resources Technical Standards

Vendor	Product	Function	Judiciary Deployment Platform	Scope
PeopleSoft		Human Resources	HP-UX	HRMIS
<a href="#">AMS</a>	Momentum	Accounting	X-86 based, Linux	FAS <sup>1</sup> CJA <sup>2</sup>

<sup>1</sup> FAS4T COTS Product

<sup>2</sup> CJA COTS Product

#### 4.7.2 Library Interchange Standards

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.3 Unicode Standards

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.4 Markup Languages

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

##### 4.7.4.2 Extensible Markup Language (XML)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.5 Portable Document Format (PDF)

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Adobe Systems</a>	Acrobat 6	Convert documents into PDF format, create interactive .pdf documents, create index, searchable, .pdf document collections	X-86 based workstation, MS Windows 2000, XP	
<a href="#">Adobe Systems</a>	Acrobat Reader 6	Freeware PDF viewer	X-86 based workstation, Linux, MS Windows 2000, XP	

#### 4.7.6 File Compression Formats

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.7 Office Automation File Formats

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Corel</a>	Corel WordPerfect 8 / 9 / 10 / 11	Word processing	X-86 based workstation, MS Windows 2000, XP	
<a href="#">Microsoft</a>	Microsoft Word XP	Word processing	X-86 based workstation, MS Windows 2000, XP	

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Microsoft</a>	Microsoft Excel XP	Spreadsheet	X-86 based workstation, MS Windows 2000, XP	
<a href="#">Microsoft</a>	Microsoft PowerPoint XP	Presentation	X-86 based workstation, MS Windows 2000, XP	
<a href="#">Microsoft</a>	Microsoft Access XP	Desktop database	X-86 based workstation, MS Windows 2000, XP	

#### 4.7.8 Calendar Date and Ordinal Date Interchange Format

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.9 Vector Graphics

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.10 Raster Image Interchange

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.11 Tagged Image File Format (TIFF)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.12 Joint Photographic Experts Group (JPEG)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.6.13 Motion Picture Experts Group (MPEG)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.14 Electronic Data Interchange (EDI)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.7.15 Computer-Aided Design (CAD) Data

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### **4.8 Graphics Services**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### **4.9 Computer-Based Interactive Training**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### **4.10 Output Services**

##### **4.10.1 Facsimile Transmission Service (fax)**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

##### **4.10.2 Compact Disk-Read Only (CD-ROM) Generation Service**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

##### **4.10.3 Digital Versatile Disc (DVD) Generation Service**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

##### **4.10.4 Digital Video and Film Generation Service**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

##### **4.10.5 Magnetic Tape Generation Service**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

##### **4.10.6 Plotting Service**

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.10.7 Print Service

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

### 4.11 Network Services

#### 4.11.1 National Internet Gateways

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T1/T3	Internet Gateway	DCN WAN	ALL
<a href="#">Cisco</a>	Routers	Internet Gateway	Cisco switches, routers	ALL

#### 4.11.2 DCN

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T1/T3	DCN WAN	DCN WAN	ALL
<a href="#">Cisco</a>	Routers	DCN WAN	Cisco switches, routers	ALL

#### 4.11.3 PacerNet

Vendor	Product	Function	Judiciary Platform	Scope
FTS2001	T1/T3	PacerNet	DCN WAN	ALL
<a href="#">Cisco</a>	Routers	PacerNet	Cisco switches, routers	ALL

#### 4.11.4 Network File and Print Services

Vendor	Product	Function	Judiciary Platform	Scope
Open Source	SSH	File services	X86 based server	ALL

#### 4.11.5 Directory and Naming Services

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">IBM/ Lotus Development Corp.</a>	Domino	Email directory	Notes Server	ALL

#### 4.11.6 Domain Name Service (DNS)

Vendor	Product	Function	Judiciary Platform	Scope
OS Vendor	Bind	DNS server	X86-based server	ALL

#### 4.11.7 Electronic Mail and Message Services

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Sendmail</a>	Sendmail	Internet Email gateway	X86-based server	ALL
<a href="#">IBM</a> / Lotus Development Corp	Notes	Internal Mail	X86-based server	ALL

#### 4.11.8 Time Service

Vendor	Product	Function	Judiciary Platform	Scope
Cisco	Cisco IOS	Time service	Cisco router	ALL

#### 4.12 Videoconferencing

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.13 Virtual LAN (VLAN)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.14 Voice Over IP (VoIP)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.15 Communication Protocols

##### 4.15.1 Internetwork Packet Exchange / Sequenced Packet Exchange (IPX/SPX)

Vendor	Product	Function	Judiciary Platform	Scope
		IPX/SPX to be phased out		

##### 4.15.2 Transmission Control Protocol / Internet Protocol (TCP/IP)

Vendor	Product	Function	Judiciary Platform	Scope
OS Vendor	TCP/IP	Default communication protocol	All	ALL

### 4.15.3 Ethernet

Vendor	Product	Function	Judiciary Platform	Scope
	IEEE802.3z	LAN protocol	All	ALL

#### 4.15.3.1 Gigabit Ethernet

Vendor	Product	Function	Judiciary Platform	Scope
	IEEE 802.3z	LAN protocol	All	ALL

### 4.15.4 Wireless Local Area Network (WLAN)

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Wireless LAN	Wireless LAN	All

### 4.15.5 Frame Relay

Vendor	Product	Function	Judiciary Platform	Scope
Sprint	FTS2001	Data Communications	DCN WAN	ALL

### 4.15.6 Asynchronous Transfer Mode (ATM)

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data Communications		

#### 4.15.6.1 LAN Emulation (LANE)

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data Communications		

#### 4.15.6.2 Emulated LAN (ELAN)

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data Communications		

#### 4.15.6.3 Multi-Protocol Over ATM (MPOA)

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Data Communications		

#### 4.15.7 Dynamic Host Configuration Protocol (DHCP)

Vendor	Product	Function	Judiciary Platform	Scope
	LAN switches and routers	DHCP Server	LAN	Local
OS Vendor	DHCP	DHCP Server	X86 based server	Local

#### 4.15.10 Multipurpose Internet Mail Extensions (MIME)

Vendor	Product	Function	Judiciary Platform	Scope
Sun	Solaris (mail server)	Internet E-Mail gateway	Sun SPARC	AO <sup>1</sup>
<a href="#">IBM</a> / Lotus Development Corp.	Notes	E-Mail	Lotus Notes server	ALL

<sup>1</sup> AO (IMD)

### 4.16 Security Services

#### 4.16.1.1 Secure Firewall

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	PIX	Firewall Security	Internet Gateway	ALL
Novell	Bordermanager	Firewall Security	N/A	ALL

#### 4.16.1.2 Intrusion Detection

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">ISS</a>	RealSecure Product suite	Network and host-based intrusion detection	Internet Gateway	ALL

#### 4.16.2.1 Authentication Protocols (PAP, CHAP, and MS-CHAP)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.16.2.2 Access Authentication Protocols (RADIUS and TACACS+)

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	RADIUS	Authentication	All	ALL

#### 4.16.3 Access Control

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Access control and authentication	All	ALL

##### 4.16.3.1 Password Usage

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

#### 4.16.4.3 Virtual Private Network (VPN)

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Cisco</a>	Cisco VPN 3000 series hardware	Remote access Virtual Private Network (VPN) platforms and client software	Remote Access	ALL
<a href="#">Cisco</a>	Cisco VPN 3000 client	Remote access Virtual Private Network (VPN) client software	X-86 based workstation	ALL

#### 4.16.4.4 Virus Control

Vendor	Product	Function	Judiciary Platform	Scope
<a href="#">Symantec Corporation</a>	Norton AntiVirus	Server and workstation virus scan software	X86 based systems	ALL

##### 4.16.4.5.2 Digital Certificate Authentication (x.509)

Vendor	Product	Function	Judiciary Platform	Scope
Verisign	Verisign	X.509 certificates	X86 based systems	ALL

### 4.17 System and Network Management Services

#### 4.17.1 Network System Administration

Vendor	Product	Function	Judiciary Platform	Scope
TBD		System Management, including distributing software	ALL	

#### 4.17.2 Help Desk Administration

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Help desk tool which supports remote location help desk operation, operations status, reports	X86 based system	ALL

#### 4.17.3 Communication Network Management

Vendor	Product	Function	Judiciary Platform	Scope
	TBD	Enterprise mapping, configuration, backup, and deployment of software to routers and switches		ALL
	TBD	Network performance and problem monitoring, mapping	X-86 based workstations	ALL
	TBD	Fault management, high level configuration management, and performance management		ALL
	TBD	Monitoring the traffic load on network		ALL

#### 4.17.4 Server Management

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Fault management process and workflow, Efficient event management, with customizable event filtering and consolidation	X86 based server	ALL

#### 4.17.5 Capacity Planning and Performance Management

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Web statistical analysis tool	X86 based server	ALL

#### 4.17.6 Backup and Recovery Service

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Backup and recovery for individual Novell NetWare and Microsoft NT / 2000 servers	X86 Based servers	ALL

### CHAPTER 5- EXTERNAL ENVIRONMENT

#### 5.2 User Desktop Workstations

Vendor	Product	Function	Judiciary Platform	Scope
TBD	The judiciary has BPAs with Dell, Compaq (HP), Gateway, and Micron.	Desktop	X-86 based workstation	ALL

#### 5.3 Information Exchange Media

##### 5.3.2 Tape

Vendor	Product	Function	Judiciary Platform	Scope
TBD		Backup Device	X-86 based server	ALL

##### 5.3.3 CD-ROM Server and Magnetic Optical Disk

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

### 5.3.4 Digital Versatile Disc (DVD) Generation Service

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

### 5.3.5 Scanners

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

## 5.4 Output Devices

### 5.4.2 Printers

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

## 5.5 Information Storage

### 5.5.2 Server Attached Local Disk Array

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

### 5.5.3 Network Attached Storage (NAS)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

### 5.5.4 Storage Area Networks (SAN)

Vendor	Product	Function	Judiciary Platform	Scope
TBD				

## 5.6 Communications Hardware

### 5.6.1 Cables

Manufacturer	Product	Model	Function	Scope
	AWG24 Category 5E 4 pair	Copper unshielded twisted pair	Cable	ALL
	Micron 8.2/125	Fiber Optics (for singlemode)	Cable	ALL

Manufacturer	Product	Model	Function	Scope
	Micron 62.5/125	Fiber Optics (for multimode)	Cable	ALL

### 5.6.2 Bridges, Routers, and Switches

Vendor	Product	Model	Function	Scope
<a href="#">Cisco</a>	Router	1000 series	Router	ALL
<a href="#">Cisco</a>	Router	2000 series	Router	ALL
<a href="#">Cisco</a>	Router	3000 series	Router	ALL
<a href="#">Cisco</a>	Router	4000 series	Router	ALL
<a href="#">Cisco</a>	Router	5000 series	Router	ALL
<a href="#">Cisco</a>	Router	6000 series	Router	ALL
<a href="#">Cisco</a>	Router	7000 series	R outer	ALL

### 5.7 Satellite Broadcasting / FJTN

Vendor	Product	Model	Function	Scope
	GE-3	Ku band antennas and receivers	Satellite Communications	ALL

## **APPENDIX D    SDSD RAID STANDARDS**

### **D.1    RAID Standards**

This appendix establishes standards for configuring the following Redundant Array of Independent Disks (RAID) distributed by the AO:

- Level 1 (RAID 1)
- Level 5 (RAID 5)

The standards in this document are designed to meet the unique requirements of each application while ensuring consistency within the Judiciary. System managers and system administrators who are responsible for server maintenance should use this document as a guide when configuring disks for the following applications:

- Case Management/Electronic Case Files (CM/ECF)
- Probation/Pretrial Automated Case Tracking System (PACTS)
- Jury Management System (JMS)
- Financial Accounting System for Tomorrow (FAS4T)

This appendix does not cover legacy systems, such as the Integrated Case Management System (ICMS) and the Court Financial System (CFS).

### **D.2    Disk Configuration Standards**

This section describes standards for physical disk placement, disk arrays, and data location.

#### **D.2.1    Physical Disk Placement**

Follow the standards in this section when physically connecting disks in an array.

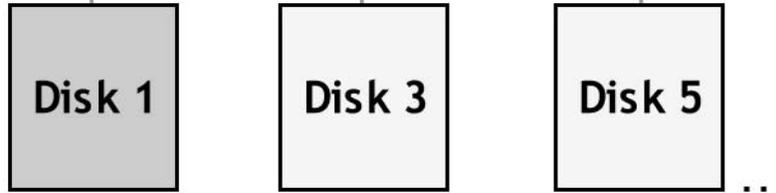
##### **D.2.1.1    Root Storage Array**

Physical disks for the root storage disk array are distributed across separate Small Computer System Interface (SCSI) channels.

##### **D.2.1.2    Application Server Storage Array**

Application disk arrays are alternated across SCSI channels. Figure D-1 depicts this arrangement.

## SCSI 1



## SCSI 2

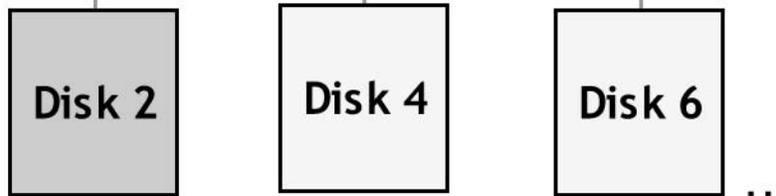


Figure D-1: Disk Placement in Storage Array<sup>4</sup>

### D.3 RAID 5

The disk configuration may include hard disks configured as RAID 5. This section describes the standards that apply to RAID 5.

#### D.3.1 Minimum and Maximum Disks

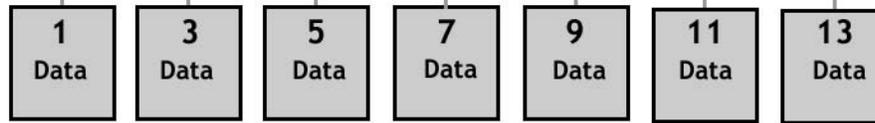
The array includes at least 4 disks, but no more than 13 disks, plus a hot spare.

Exception 1 applies to this standard. The total disk capacity in the array cannot exceed 500 GB. When calculating the disk capacity, remember that one disk is used for data parity and is not included in the total. For example, in an array of 13 disks, an amount of space equivalent to the size of one disk is used for parity and not included when calculating the approximate size of the array. For an array of 13 36-GB disks, the approximate size of the array is 432 GB (12 x 36).

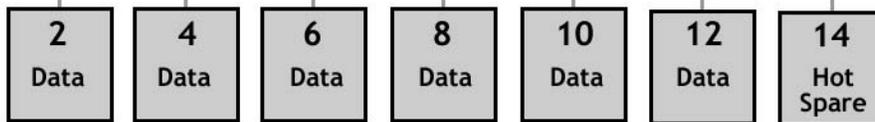
#### D.3.2 Hot Spare

As shown in Figure D-2, one hot spare should be added to a RAID 5 array. The location of the hot spare in the array is unimportant.

## SCSI 1



## SCSI 2



**Figure D-2: Example of Hot Spare Configuration**

### D.3.3 Location

The following factors determine whether the disks that compose the array are located inside the system or in an external chassis:

- Number of disks
- Technical and physical limitations of the system Exception 1 on page 2 applies to the RAID 5 standards in this section.

### D.4 Data Configuration Standards

This section describes standards for the placement of data and software.

#### D.4.1 Data Placement

The standards in this section specify where data should be stored.

##### D.4.1.1 Root Disk

The root disk is for the operating system (OS) and AO-supplied packages only. Do not store court or vendor applications on the root disk.<sup>5</sup>

##### D.4.1.2 /usr

The /usr file system contains only OS binaries and OS scripts.

##### D.4.1.3 /gov

The /gov file system contains applications and utilities supplied by the AO, such as gzip and Perl. Exceptions 2 (above) and 3 (below) apply to this standard.<sup>6</sup>

#### D.4.1.4 Packaging

All AO and vendor-distributed application and utility server-based software are packaged using the Solaris suite of standard application packaging utilities.

#### D.4.2 Software Standards

This section describes standards for software supplied by the AO and by vendors.

##### D.4.2.1 Application Logs

Application logs are written to the `/var/log/app_name/service/logname` file using the values described in Table D-1.

**Table D-1: Values in the Application Log Directory Structure**

Value	Description
<code>app_name</code>	Name of the application that generates the logs. Examples: FAST, JMS, ECF, ECM, Tuxedo, or Informix
<code>service</code>	Any subdirectory that clarifies <code>app_name</code> (at the developer's discretion). Examples: Production, Live, Test, or Train
<code>logname</code>	Unique name of the log

##### D.4.2.2 Start/Stop Scripts

The run control scripts in `/etc/rc#.d` link to application start/stop scripts stored in `/etc/init.d`.

##### D.4.2.3 Path Names

Scripts use relative path names. Whenever possible, configuration files use variables to declare path names.

##### D.4.2.4 Symbolic Links

Scripts may point to the current version of an application using a symbolic link name that meets the following criteria:

- Contains less than 15 characters
- Avoids naming conflicts
- Resides in an appropriate `Application_Software_Directory` (see examples at the end of this document)

##### D.4.2.5 Local Applications

At the discretion of the system administrator, local applications are installed in the `/usr/local` directory. Only applications that the system administrator has deemed to be local should be installed in the `/usr/local` directory.

Exception 3 on page 4 applies to local applications.

## D.5 Server Configuration Standards

This section specifies how disk storage is allocated on servers.

### D.5.1 CM/ECF Outside Server

Root storage on the CM/ECF outside server uses either two 9.1-GB or two 18-GB disks in a RAID 1 configuration. Assign additional free space as noted in Table 2 or Table 3. Because this is a single-array configuration, the /app01 mount point must reside on the root disk.

#### D.5.1.1 9.1-GB Disks

Table D-2 identifies how hard disk space is allocated for 9.1-GB disks.

**Table D-2: Hard Disk Configuration for 9.1-GB Disks**

Mount point	Disk space allocation
/	700 MB
swap	2000 MB
/usr	1322 MB
/var	1322 MB + 10% of remaining space
/gov	900 MB + 10% of remaining space
/tmp	1024 MB
/app01	1274 MB + 80% of remaining space

#### D.5.1.2 18-GB Disks

Table D-3 identifies how hard disk space is allocated for 18-GB disks.

**Table D-3: Hard Disk Configuration for 18-GB Disks**

Mount point	Disk space allocation
/	1024 MB
swap	2048 MB
/usr	3072 MB
/var	4096 MB
/gov	2048 MB
/tmp	1920 MB
/app01	3072 MB + remaining space

### D.5.2 Application Server Storage Array(s)

This section describes storage guidelines for the root and application disks of an application server.

### D.5.2.1 Root Storage

Application servers use either two 9.1-GB or two 18-GB disks in a RAID 1 configuration for root storage. Assign additional free space as noted in Table D-4 or Table D-5.

### D.5.2.2 9.1-GB Disks

Table D-4 identifies how root space is allocated for 9.1-GB disks.

**Table D-4: Root Space Allocation for 9.1-GB Disks**

Mount point	Disk space allocation
/	700 MB + 10% of remaining space
swap	2000 MB
/usr	2048 MB
/var	1322 MB+ 10% of remaining space
/gov	1200 MB + 80% remaining space
/tmp	1024 MB
/home	250 MB

### D.5.2.3 18-GB disks

Table D-5 identifies how root space is allocated for 18-GB disks.

**Table D-5: Root Space Allocation for 18-GB Disks**

Mount point	Disk space allocation
/	1024 MB
swap	2048 MB
/usr	3072 MB
/var	4096 MB
/gov	2048 MB + remaining space
/tmp	3072 MB
/home	1920 MB

### D.5.3 Application Storage

Table D-6 defines the minimum number of disks and the RAID configuration used by each application. Allocate all available space to the mount points listed in either Table D-4 or Table D-5.

**Table D-6: Application Directory Space Allocation**

<b>Mount point</b>	<b>Application</b>	<b>Min. # disks</b>	<b>RAID</b>
/app01	FAS4T JMS CM/ECF PACTS	3 2	5 1
/app02	CM/ECF PACTS	2	1
/app03	CM/ECF	4	5

## **D.6 Application Storage Directory Standards**

The following components are located in the /app## directories:

- Informix Relational Database Management System (RDBMS)
- Application software
- Databases and data files

### **D.6.1 Required Directory Structure**

The following example illustrates the required directory structure for an application:

**/app##**

**/Application\_Software\_Directory** (if applicable)

**/phase** or **/version** (whichever is applicable)

**/db01**

**/Application\_Software\_Directory**

**/version** (if applicable)

**/phase**

Table D-7 defines the values used in the previous example.

**Table D-7: Values in the Required Directory Structure**

<b>Value</b>	<b>Description</b>
<b>/app##</b>	Single-mount point for the RAID ( <b>##</b> is a two-digit number representing the number of the array where 01 is the first array). Examples: app01, app02, and so on.
<b>Application_Software_Directory</b>	Application name specified by the vendor. Examples: DCECF, pactsecm, FAS4T, JMS, Tuxedo, Informix, and others.
<b>phase</b>	Any subdirectory that clarifies the <i>Application_Software_Directory</i> . Examples: Production, Live, Test, and Train (if necessary).
<b>version</b>	Any subdirectory that clarifies the <i>Application_Software_Directory</i> (use is at the discretion of the developer). Examples: 3.5.0.10 for FAS4T or 7.31.4 for Informix

Examples of directory structures for specific applications are shown on the following pages. The application developer, distribution manager, and application support manager may designate the directory structures beneath the required directories.

NOTE: In the examples that follow, required directories appear in bold type. When creating a directory structure, use the exact names shown for these required directories. However, you may name optional directories and files as you wish. In the examples, optional directories and files are provided for clarity and appear in roman type.

## D.6.2 JMS /app01 Directory

The following example shows the **/app01** directory structure and files on a JMS application server:

### **/app01**

**/informix** (Example: currentjms => symbolic link to the current version of Informix)

**/7.31.4**

**/aaodir**

**/bin**

...

### **/JMS**

**/live**

jurfeds.sh

juryprod.sql

jurytrain.sql

...

### **/db01**

**/JMS**

**/live**

jms\_datachk1

jms\_idxchk1

...

### D.6.3 FAS4T /app01 Directory

The following example shows the /app01 directory structure and files on a FAS4T application server:

```
/app01  
  /tuxedo  
    /6.3  
      /apps  
      ...  
    /6.4  
      /apps  
      ...  
  /informix  
    /7.31.4  
      /aadir  
      /bin  
      ...  
  /FAS4T (Example: fastcurrent => symbolic link to the current version of FAS4T)  
    /3.5.0.10  
    ...  
  /db01  
    /FAS4T  
      /3.5.0.10  
        /prod  
          chunk_proddata1  
          ...  
        /test  
          chunk_testdata1  
          ...  
        /train  
          chunk_traindata1  
          ...
```

#### D.6.4 CM/ECF /app## Directory

The following example shows the /app## directory structure and files on a CM/ECF application server. Replace *courtID* with your court's ID—for example, txwb.

```
/app01  
  /stronghold (Apache Stronghold version 3)  
  ...  
  
  /informix (Example: currentecf => symbolic link to the current version of Informix)  
    /7.31.4  
      /aaodir  
      /bin  
      ...  
  
  /BKECF or /DCECF or /ACECF (whichever is applicable)  
    /live  
      /server  
      /web  
      ....  
    /test  
      /server  
      /web  
      ...  
    /train  
      /server  
      /web  
      ...  
  
/db01  
  /ECF  
    /live  
      courtID_root  
      courtID_temp1  
      courtID_db1  
      ...  
    /test  
      courtIDtest_db1  
      ...  
    /train  
      courtIDtrain_db1  
      ...
```

**/app02**

**/db01**

**/ECF**

**/live**

courtID\_temp2

courtID\_db2

...

**/test**

courtIDtest\_db2

...

**/train**

courtIDtrain\_db2

...

**/app03**

**/db01**

**/ECF**

**/live**

/docs

...

**/test**

/docs

...

**/train**

/docs

...

### D.6.5 PACTS /app## Directory

The following example shows the /app## directory structure on a PACTS application server:

#### /app01

**/informix** (Example: current => symbolic link to the current version of Informix)

**/7.31.4**

  /aaodir

  /bin

  ...

**/pactsecm**

  /devl

  /prod

  /train

  ...

**/db01**

  /pactsecm

    /bkup

    ...

**/app02**

  /db01

    /pactsecm

      /photos

      ...

## **APPENDIX E    WORKSTATION CONFIGURATIONS**

### **E.1    Minimum Client Hardware Requirements**

#### **E.1.1    Light Client (e.g., browser interface)**

Windows 2000 or XP  
Intel Pentium 200 MHz (or equivalent) CPU  
256 Mb RAM  
100 Mbytes free space  
15" SVGA color monitor  
Mouse  
NIC (network card)

#### **E.1.2    Medium Client (e.g., browser with active components)**

Windows 2000 or XP  
Intel Pentium 400 MHz (or equivalent) CPU  
512 Mb RAM  
100 Mbytes free space  
15" SVGA color monitor  
Mouse  
NIC (network card)

#### **E.1.3    Heavy Client (e.g., application on client with network access to database or backend)**

Windows 2000 or XP  
Intel Pentium 1 GHz (or equivalent) CPU  
512 Mb RAM  
500 Mbytes free space  
15" SVGA color monitor  
Mouse  
NIC (network card)

In general, greater CPU power, memory, free space, and resolution of monitor are also acceptable.

## APPENDIX F    ACRONYMS

3DES	Triple-Data Encryption Standard
ACL	Access Control Lists
AD	Active Directory (Microsoft)
AES	Advanced Data Encryption
AIIM	Association for Information and Image Development
AIS	Automated Information Systems
ALA	American Libraries Association
ANSI	American National Standard Institute
API	Applications Program Interface
APP	Application Portability Profile
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BISDN	Broadband Integrated Services Digital Network
BUS	Broadcast and Unknown Server
CA	Certificate Authority
CA	Collision Avoidance
CAD	Computer-Aided Design
CAE	Computer Aided Engineering
CAM	Computer Aided Manufacturing
CASE	Computer Aided Software Engineering
CAT	Control and Analysis Tool
CCITT	Consultative Committee for International Telephony and Telegraphy (now International Telecommunications Union [ITU])
CD	Collision Detection
CD-ROM	Compact Disk Read Only Memory
CDS	Classified Data System
CGM	Computer Graphics Metafile
CHAP	Challenge Handshake Authentication Protocol
CIT	Information Technology Committee
CLI	Command Level Interface
CLI	Call Level Interface
CM	Configuration Management
CM/ECF	Case Management/Electronic Cases Files
CORBA	Common Object Request Broker Architecture
COS	Classes Of Service
COTS	Commercial Off The Shelf Software
CPDF	Central Personnel Data File
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CRT	Cathode Ray Tube

CSE	Communication Security Establishment (Canada)
CSMA	Carrier Sense Multiple Access
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSS	Cascading Style Sheet
CTO	Chief Technology Officer
CVB	Central Violation Bureau
DAC	Directory Access Control
DAP	Document Application Profile
DAP	Directory Access Protocol
DBAD	Detailed Business Area Description
DBMS	Database Management System
DCAA	Distributed Computing Applications Architecture
DCAF	Distributed Computer Architecture Framework
DCE	Distributed Computing Environment
DCN	Data Communications Network
DCOM	Distributed Component Object Model
DCT	Discrete Cosign Transformation
DES	Data Encryption Standard
DFD	Data File Delivery
DFS	Distributed File Service
DHCP	Dynamic Host Configuration Protocol
DISA	Data Interchange Standards Association
DMA	Document Management Alliance
DMZ	De-Militarized Zone
DNS	Domain Name Service
DSA	Digital Standard Algorithm
DSS	Digital Signature Standard
DSSS	Direct Sequence Spread Spectrum
DTD	Document Type Definition
DVD	Digital Versatile Disk
EBI	Enterprise Business Intelligent
ECC	Error Correction Code
EDAP	Extended Data Availability and Protection
EDI	Electronic Data Interchange
EDIFACT	EDI for Administration, Commerce, and Transport
EDMS	Executive Document Management System
EEI	External Environment Interface
EFI	Electronic Funds Transfer
EGP	Exterior Gateway Protocol
EJB	Enterprise Java Beans
EIS	Executive Information System
ELAN	Emulated Local Area Network
EMS	Enterprise Mail gateway System
ERD	Entity Relationship Diagram
ERM	Electronic Records Management
FASAB	Federal Accounting Standards Advisory Board

FAS4T	Financial Accounting System for Tomorrow
FC-AL	Fiber Channel-Arbitrated Loop
FCR	First Call Resolution
FDDI	Fiber Distributed Data Interface
FDRD	Functional and Data Requirements Definition
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
FJTN	Federal Judiciary Television Network
FRAD	Frame Relay Access Device
FRS	Frame Relay Service
FTP	File Transfer Protocol
GKS	Graphical Kernel Services
GUI	Graphical User Interface
HLA	High Level Architecture
HPUX	Hewlett Packard Unix
HRMIS	Human Resource Management Information Systems
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
I-CASE	Integrated Computer Aided Software Engineering
ICMS	Integrated Case Management Systems
ICOM	Inputs, Controls, Outputs, and Mechanisms
ICMP	Internet Control Message Protocol
ICSA	International Computer Security Association
IDE	Integrated Data Environment
IDEA	International Data Encryption Algorithm
IDMEF	Intrusion Detection Message Exchange Format
IDS	Intrusion Detection System
IDWG	Intrusion Detection Working Group
IDXP	Intrusion Detection Exchange Protocol
IEEE	Institute of Electrical and Electronic Engineers
IEF	Information Engineering Facility
IETF	Internet Engineering Task Force
IGES	Institute for Global Environmental Strategies
IGRP	Interior Gateway Routing Protocol
IIOP	Internet Inter-Orb Protocol
ILE	Integrated Library System
IP	Internet Protocol
IPX	Internet Packet Exchange
IPX	Inter-network Packet Exchange
IR	Infrared light
IRD	Integrated Receiver Decoder
IRDS	Information Resource Dictionary System
IRMS	Information Resources Management Standard
ISA	Information Systems Architecture
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System

ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITPMP	Information Technology Project Management Process
ITU	International Telecommunications Union
J2EE	Java™ 2 Platform, Enterprise Edition
JDBC	Java Database Connectivity
JFMIP	Joint Financial Management Improvement Program
JPEG	Joint Photographic Experts Group
JMS	Jury Management System
JNET	Judiciary NET
LAN	Local Area Network
LANE	Local Area Network Emulation
LCD	Liquid Crystal Display
LCM	Life Cycle Management
LDAP	Lightweight Document Application Profile
LE	Life Expectancy
LEC	LAN Emulation Clients
LEC	LAN Emulation Configuration Server
LES	LAN Emulation Server
MAC (address)	Media Access Control (address)
MAN/LAN	Metropolitan Area Network/Local Area Network
MARBI	Machine-Readable Bibliographic Information (American Library Association)
MARC	Machine-Readable Cataloging (U.S. Library of Congress)
MDDBMS	Multidimensional Database Management Systems
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
M-O	Magneto-Optical (disks)
MPEG	Motion Picture Experts Group
MPLS	Multi-Protocol Label Switching
MPOA	Multi-Protocol Over ATM
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NAS	Network Attached Storage
NAT	Network Address Translation
NDMP	Network Data Management Protocol
NDS	Novell Directory Services
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIBS	National Integrated Bankruptcy System
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NOS	Network Operating Systems
NSA	National Security Agency
NTIS	National Technical Information Service

NTP	Network Time Protocol
OCLC	Online Computer Library Center
ODA	Open Document Architecture
ODBC	Open Database Connectivity
ODMA API	Open Document Management Applications Program Interface
OIT	Office of Information Technology
OLAP	Online Analytical Processing
OLTP	Online Transaction Processing
OMG	Open Group Management
OMG IDL	Open Group Management Interface Definition Language
OS	Operating System
OSE	Open System Environment
OSI	Open System Interconnection
OSPF	Open Shortest Path First
OTM	Object Transaction Monitor
FACTS	Probation and Pre-Trial Offices Services Automated Case Tracking System
PAP	Password Authentication Protocol
PCO	Project Coordination Office
PDF	Portable Document Format
PEN	Polyethylene Napthalene
PET	Polyethylene Terephthalate
PIX	Private Internet Exchange
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
POSIX	Portable Operating System Interface for Computer Environment
PVC	Private Virtual Circuits
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RAS	Remote Access Server
RCA	Root Call Analysis
RDA	Remote Database Access
RDBMS	Relational Database Management Systems
RDF	Resource Description Framework
RE-TM	Rare Earth Transition Metal
RF	Radio Frequency
RFC	Requests For Comments
RIP	Routing Information Protocol
RISC	Reduced Instruction Set Computer
RLE	Run-Length Encoding
RLIN	Research Libraries Information Network
RM	Requirements Management
RMI	Remote Method Invocation
ROLAP	Relational Online Analytical Processing Servers

RPC	Remote Procedure Call
RSA	Rivest Shamir Adleman
RTF	Rich Text Format
RTM	Requirements Traceability Management
SAN	Storage Area Network
SBU	Sensitive But Unclassified
SCSI	Small Computer System Interface
SESAME	Secure European System for Applications in a Multi Vendor Environment
SET	Secure Electronic Transaction
SGML	Standard Generalized Markup Language
SHS	Standard Hash Standard
S-HTTP	Secure Hypertext Transport Protocol
SITP	Strategic Information Technology Plan
SLA	Service-Level Agreements
S/MIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SoIP	Storage over IP
SPX	Sequence Packet Exchange
SQL	Structured Query Language
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control System
TAG	Technical Advisory Group
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIFF	Tag Image File Format
TLS	Transport Layer Security
TOG	The Open Group
TP	Transaction Processing (monitors)
TPM	Transaction Processing Monitoring
TQM	Total Quality Management
TRM	Technical Reference Model
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modeling Language
URI	Uniform Resource Identifiers
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair
VoIP	Voice over Internet Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAIS	Wide Area Information Server
WAN	Wide Area Network

WAS	Web Application Servers
WCM	Web Content Management
WebDAV	World Wide Web Distributed Authoring and Versioning
WLAN	Wireless Local Area Network
WORM	Write Once, Read Many (disk)
WSDL	Web Service Description Language
WWW	World Wide Web
XDR	External Data Representation
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language
XSLT	Extensible Stylesheet Language Transformations

## APPENDIX G REFERENCES

Many references were identified in footnotes throughout the entire document.

1. National Institute of Standards and Technology. *Application Portability Profile (APP)*. The U.S. Government's Open Systems Environment Profile Version 3.0, NIST Special Publication 500-230. February 1996.
2. National Institute of Standards and Technology. *Integration Definition for Function Modeling (IDEF0)*. FIPS 183. December 21, 1993.
3. Open Systems Environment Architectural Framework for National Information Infrastructure Services and Standards. Draft 1.0. August 5, 1994.
4. Patent and Trademark Office. *Life Cycle Management for Automated Information Systems Overview*. December 1997.
5. Patent and Trademark Office. *United States Patent and Trademark Office Strategic Information Technology Plan for Fiscal Years 1999-2004*.
6. Patent and Trademark Office. *United States Patent and Trademark Office Technical Reference Model Version 6.0*.
7. A Practical Guide to Federal Enterprise Architecture, Chief Information Officer Council, Version 1.0, February 2001.
8. Federal Enterprise Architecture Framework, Version 1.1, September 1999, CIO Council.
9. Architecture Alignment and Assessment Guide, October 2000.
10. Smithsonian Institution. Technical Reference Model, Version 2.0, February 2003.