

# **Supreme Court of Florida Office of the State Courts Administrator**

---

## **Integration and Interoperability Document**

---

**Version 2.1**

**5 May 2011**



## Revision History

Date	Version	Changed By	Notes
08/27/2002	1.0	M. Ervin	First edition of the Interoperability & Integration Requirements Document
09/12/2002	1.1	M. Ervin	Incorporated comments from OSCA review
10/02/2002	1.2	M. Ervin	Incorporated comments from CTOs' review
10/09/2002	1.3	M. Ervin, OSCA	Additional refinement of document for release
10/28/2004	1.4	CTO Workgroup	Annual Review and Update
11/05/2004	1.5	OSCA	Final Draft
11/15/2004	1.6	Gary Hagan	Update Wire Section
11/16/2004	1.7	OSCA	Update XML Specifications
07/10/2007	1.8	I&I Workgroup	
03/19/2008	1.9	Jannet Lewis	Updated Network Diagrams MFN Network
4/29/2011	2.0	Technical Standards Committee	Updated entire document
5/5/2011	2.1	Lakisha Hall	Updated Desktop Standards section as a result of the FCTC May 4, 2011 meeting

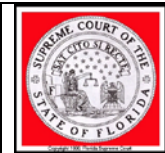


## Table of Contents

1. Overview .....	4
2. Background .....	4
3. Requirements and Standards for Integration & Interoperability .....	4
3.1 Diagrams .....	4
3.2 Integration Requirements and Standards .....	7
3.2.1 Infrastructure Standards and Requirements .....	7
3.2.2 Security Standards .....	15
3.2.3 System Management Tools .....	17
3.2.4 Audio and Video Teleconferencing .....	18
3.2.5 Court Reporting Technologies .....	19
3.2.6 Technical Support .....	19
3.2.7 Courtroom Technology Standards .....	20
3.3 Requirements for Interoperability and Data Exchange Standards .....	22
3.3.1 Data Exchange Standards (eXtensible Markup Language (XML)) .....	24
3.3.2 Database Standards .....	26
3.3.3 Database Connectivity .....	27
3.4 Cloud Computing .....	28
3.4.1 Definition of Cloud Computing .....	28
3.4.2 Characteristics of the Cloud .....	28
3.4.3 Deployment Models .....	29
3.4.4 Service Models .....	29
3.4.5 Data Protection .....	30
3.4.6 Service Level Agreement (SLA) .....	30
3.4.7 Standards Development .....	30
Appendix .....	32
Benefits of Cloud Computing .....	32
Utilizing Cloud .....	33

## Figures

Figure 1. Florida Courts Conceptual Network Design .....	5
Figure 2. Florida Courts Conceptual Circuit Network Design .....	6
Figure 3. Minimum Desktop Configurations for New Machines .....	8
Figure 4. Recommended Laptop Configurations .....	8
Figure 5. Software Requirements and Standards .....	9
Figure 6. Conceptual Data Exchange Environment .....	27



## **1. Overview**

This section contains subsections that describe the scope of the processes to which the Interoperability and Integration requirements apply.

## **2. Background**

The integration and interoperability requirements and standards are derived primarily from industry best practices and existing standards. The functional requirements of the judicial branch drive the need to define an environment that can fulfill the needs of all justice partners as they interact with the public and other federal, state, and local agencies. The hardware and software platforms, network infrastructure, and methods for data exchange that are discussed and recommended in this document support the vision of the Florida Courts Technology Commission relative to integration and interoperability among multiple heterogeneous systems.

## **3. Requirements and Standards for Integration & Interoperability**

This section contains the preliminary requirements and potential standards for interoperability and integration in the judicial branch environment. The requirements and standards were defined by analyzing functional requirements, current information architecture, and infrastructure reports, and applying that knowledge to a solution that reflects the current state of the information management industry standards and best practices for integration and interoperability.

### **3.1 Diagrams**

The diagrams in this section give an overview of the conceptual network architecture for the courts (Figure 1) and for the circuits (Figure 2).



Figure 1. Florida Courts Conceptual Network Design

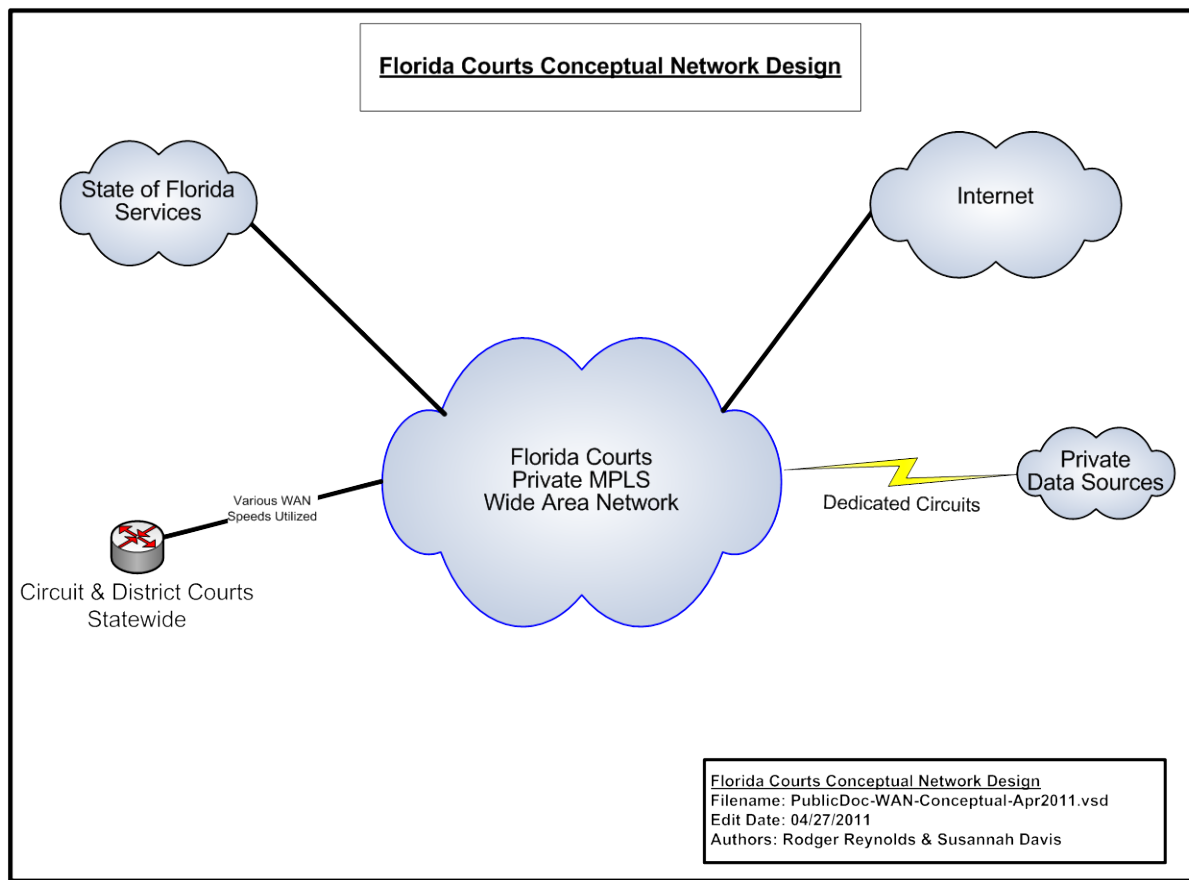
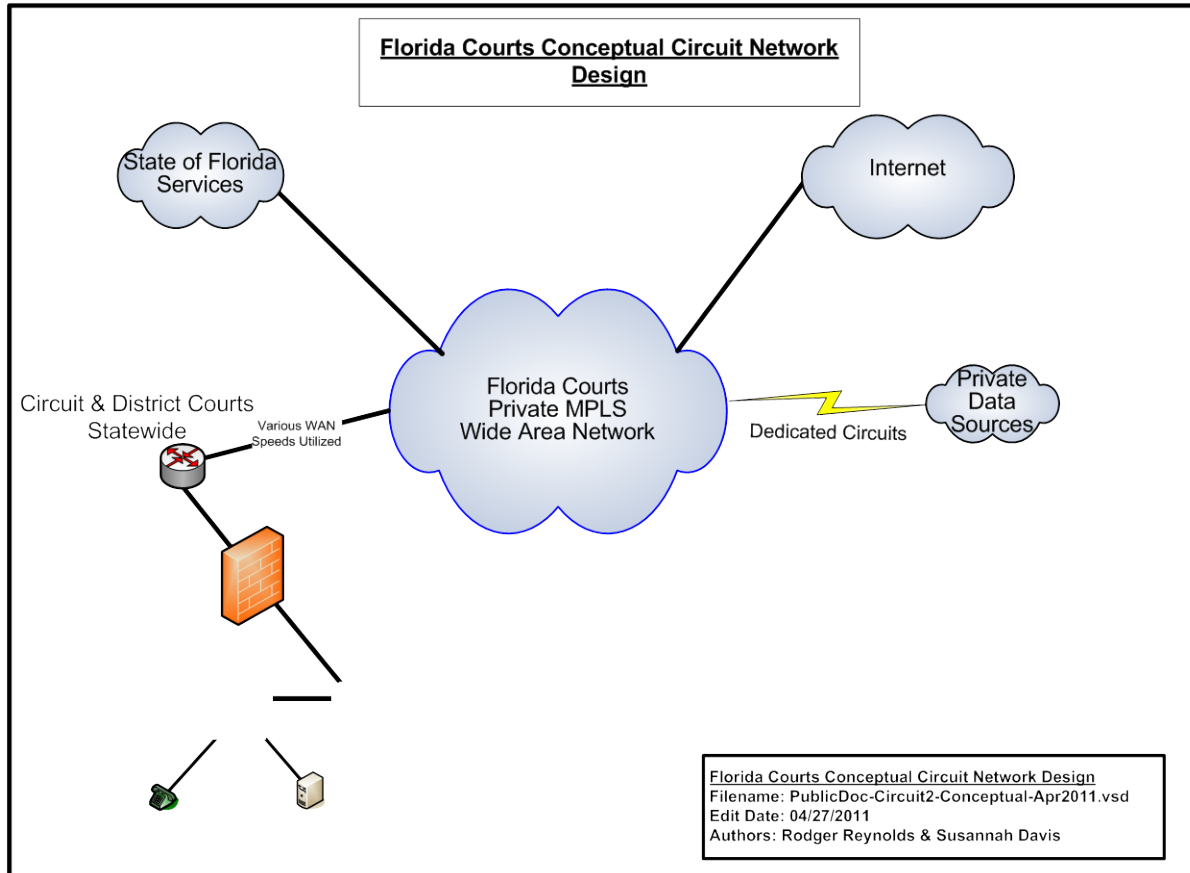
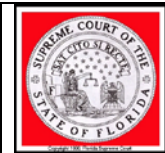




Figure 2. Florida Courts Conceptual Circuit Network Design





## **3.2 Integration Requirements and Standards**

Integration requirements and standards are needed to provide the court with an understanding of both the high-level logical design requirements and the physical infrastructure standards and requirements that will be required to efficiently integrate the disparate systems that will support the courts.

### **3.2.1 Infrastructure Standards and Requirements**

Standards and Requirements are established to provide an approach to hardware and software standardization and replacement policies that will aid in keeping technology current. Due to Florida Statutes 29.008, county(s) within each Judicial Circuit are responsible for the courts technology costs relative to computer hardware (i.e., desktops with monitors, laptops and servers, etc.) Because of technology flux and the larger issue of total cost containment, life cycle management planning is recommended. The plan should include hardware and software procurement strategies, physical asset management, technical support strategies, and retirement and disposal strategies that all enhance the attainment of organizational business objectives.

It is important to remember that the personnel costs for maintenance of computer systems are frequently greater than the hardware and system software costs. Therefore the goal of these guidelines is twofold: 1) Provide a robust infrastructure that will support the integration and interoperability of the judicial branch information systems and 2) Standardize in order to save money due to economies of scale.

#### **3.2.1.1 Desktop Standards**

Personal Computer (PC) procurements are expected to achieve certain life cycle and performance objectives. In general, a three or four-year asset life cycle is recommended. The minimum and recommended performance level requirements for desktops currently are listed in Figures 3 and 4. The performance level required will be determined by evaluating various criteria, including the number and types of applications being run, organizational needs, and performance expectations of the user.

#### **Courtroom/Hearing Room**

Monitors size: Courtroom and hearing room monitors shall have sufficient screen size that has the ability to display multiple electronic documents. 30" monitor or better preferred. Monitor placement should be in a manner that prevents obstruction of the judge's view of the courtroom or hearing room.

#### **Judge's Chambers**

Monitor size: 22" or greater with capability for dual monitors



**Judge’s Portable Device**

Portable devices such as tablet computers should be provided to judges to allow remote access to court files.

**Monitors**

Monitor replacement lifecycles may differ from desktop lifecycles based on functionality and usage requirements.

**Figure 3. Minimum Desktop Configurations for New Machines**

		Details
<b>Hardware</b>	<b><u>Processor</u></b>	Dual Core Business Class Intel or AMD (3.4 GHz or greater)
	<b><u>Memory (RAM)</u></b>	4 GB or Greater
	<b><u>Hard Disk</u></b>	250 GB
	<b><u>Video</u></b>	DirectX 9 or greater Capable (WDDM Driver Support recommended)
	<b><u>Monitor &amp; Graphics RAM</u></b>	Flat Panel size based on usage 256 MB or greater, system should be able to accommodate dual monitors
	<b><u>Sound</u></b>	Audio is required in accordance with planned use of the system
	<b><u>USB</u></b>	Easily accessible USB 3.0 Interface and multiple USB ports as required
	<b><u>Optical</u></b>	DVD-RW combo drive
	<b><u>Life Cycle</u></b>	3-4 Years
<b>Network Connection</b>	<b><u>High-bandwidth</u></b>	100/1000BaseT Ethernet
	<b><u>Low-bandwidth</u></b>	Wireless as required

**3.2.1.2 Laptops**

**Figure 4. Recommended Laptop Configurations**

		Details
<b>Hardware</b>	<b><u>Processor</u></b>	Dual Core Business Class Intel or AMD (2 GHz or greater)
	<b><u>Memory (RAM)</u></b>	4 GB or Greater
	<b><u>Hard Disk</u></b>	250 GB



	<b>Video</b>	DirectX 9 or greater Capable (WDDM Driver Support recommended) 256 MB (in addition to RAM)
	<b>Monitor</b>	<b>Depends on application</b>
	<b>Sound</b>	Audio required.
	<b>USB</b>	Easily accessible USB 3.0 Interface and multiple USB ports as required
	<b>Optical</b>	DVD-RW drive
	<b>Lifecycle</b>	3 years
<b>Network Connection</b>	<b>High-bandwidth</b>	Integrated 100/1000 Ethernet LAN (standard)
	<b>Low-bandwidth</b>	Integrated 56 Kbps
	<b>Wireless</b>	<b>Internal adapter supporting 802.11 b/g/n</b>

Note: In moving towards electronic documents, laptop screen size or other options for viewing should be considered.

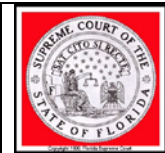
### 3.2.1.3 Client (Desktop/laptop) Software Standards

The software requirements for desktops provide a standardized environment for users. This standardization will simplify and make more efficient the initial deployment and on-going support for desktops and laptops.

<i>Figure 5. Software Requirements and Standards</i>	
<b>Software</b>	<b>Details</b>
Operating System	Windows 7
Office Suite	Microsoft Office 2007 or greater **
HTML Browser	Microsoft Internet Explorer 8 or higher
Email	Microsoft Exchange or compatible messaging system including Lotus Notes
Other Applications	1) Adobe Acrobat Reader X or other compatible PDF reader (Minimum Acrobat Reader- Other Full versions if needed) 2) Anti-virus
	<b>**Microsoft Enterprise Agreements should be considered for maximum upgrade benefits.</b>

### 3.2.1.4 Portable Devices

Portable devices for purposes of this section are devices that have computing power that allows it to access the internet, receive email, run applications on the client side, and interact with application



programs on the server side. These devices act as a portable personal computer and may include tablets, smart phones, and other similar devices. Portable devices presently have limited security features, and should be limited to less sensitive areas of access unless a specialized security measure can be applied that will meet security standards.

### 3.2.1.5 Servers

Production servers should support both common/shared services as well as organization-specific services. The proposed servers should meet a combination of priorities, including affordability, performance, scalability, space-optimization, and support for the mission-critical applications that will comprise the system.

### 3.2.1.6 Network Components

#### Courts LAN

Within each circuit or county, an internal network provides access from the judicial client to the State Network. The State Network will be the primary means used to support the transport of media among circuits.

#### *Considerations/Recommendations:*

The standard for agency LAN implementations should be established. It is recommended that the standard include the following.

- Naming conventions using DNS should be standardized across the courts
- Ethernet topology (over unshielded twisted pair cabling)
- High-speed copper (UTP) to the desktop (CAT5e or better)
  - Utilize BICSI Standards as a guideline for structural wiring
- Fiber optic cable for interconnections between high-speed concentration areas
  - Standardized connectors (ST, SC, LC, FC) and type single/multimode
- Networking equipment should be based on a full-switched TCP/IP network
  - Backbone should have Layer 3 capability for VLAN/Routing/QoS
  - Switches should have fiber uplink capability
- Scalable high speed Ethernet/Fiber switches
- Bandwidth standards and requirements within and among each judicial location are recommended at:
  - Gig to servers
  - Gig to workstations
- Use of existing LAN technology at the Judicial Locations should be evaluated on a judicial location-by – judicial-location basis and where required the LAN infrastructure should be upgraded to meet the standard.
- Any local area network technology dedicated for use by the court should follow the following requirements:

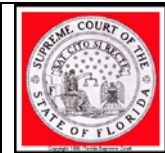
Feature Sets	IP Routing, VRRP, HSRP, STP enhancements, 802.1s/w, IGMP snooping, IEEE 802.3af Power over Ethernet (PoE).
Security	ACL, port security, MAC address notify, AAA, RADIUS/TACAC+, 802.1x,



	SSH, SNMPv3, IPv6
Advanced QoS	Layer 2–4 QoS with Class of Service (CoS)/Differentiated Services Code Point (DSCP), & Differentiated Services Model (DiffServ) supporting shaped round robin, strict priority queuing. QoS compliant with DiffServ (IETF) standards as defined in RFC 2474, RFC 2475, RFC 2597 and RFC 2598 and DSCP (IETF) standards as defined in RFC 791, 2597 2598, 2474, 3140 4594[MediaNet]. 802.1p, 802.1Q, 802.11e Resource Reservation protocol (RSVP) in RFC 2205.
Management	One IP address and configuration file for entire stack. Embedded web-based cluster management suite to Layer 2/3/4 services easy configuration of network wide intelligent services in local or remote locations automatic stack configuration.
Performance	Distributed Layer 2 and Layer 3 distributed providing <i>wire-speed</i> switching and routing via Gigabit Ethernet and Fast Ethernet configurations
Deployment	Automatic configuration of new units when connected to a stack of switches. Automatic OS version check of new units with ability to load images from master location. Auto-MDIX and Web setup for ease of initial deployment. Dynamic trunk configuration across all switch ports. Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. IEEE 802.3z-compliant 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, 1000BASE-T and CWDM physical interface support through a field-replaceable small form-factor pluggable (SFP) unit. 10 gigabit Ethernet IEEE 802.3-2008
Configuration / Survivability	Switches must work standalone and in a stacked configuration. Stack up to 9 units, Separate stacking port. Minimum 32Gbps fault tolerant bidirectional stack interconnection. Master/slave architecture with 1:N master failover . Less than 1 second Layer 2 failover with nonstop forwarding. Less than 3 second Layer 3 failover with no interrupt forwarding. Cross-stack technology, cross-stack QoS Single network instance (IP, SNMP, CLI, STP, VLAN). Minimum of 24 Ethernet 10/100/1000 ports and 2 SFP uplinks with IEEE 802.3af and pre-standard Power over Ethernet (PoE).
Interface	Must have “Cisco” compatible command-line interface (CLI)
Software	<ul style="list-style-type: none"> <li>Intelligent services: Layer 3 routing support via RIP, OSPF, static IP routing.</li> <li>Dynamic IP unicast routing, smart multicast routing, routed access control lists (ACLs), Hot Standby Router Protocol (HSRP) support and Virtual Router Redundancy Protocol (VRRP).</li> </ul>

### Courts WAN

The wide area network (WAN) infrastructure supporting the courts system will use the State Network as the primary transport media. The particular WAN hardware and software solution should be evaluated and customized to handle the additional traffic volumes that may be required from the system. Integration of local county network infrastructure to the State Network will be handled on a case-by-case basis as defined in Florida Statutes 29.008(f)(2).



### ***Considerations/Recommendations:***

- The courts should strive to standardize Domain Naming Services conventions, Network Address Translation (NAT) conventions and TCP/IP conventions (including sub netting) based on RFP standards.
- The current infrastructure supports high-speed switching technology The WAN infrastructure should include the use of TCP/IP for inter-agency communications.
- Where possible the communications infrastructure should provide for coexistence with existing architectures until these architectures can meet the standard.
- Multi-protocol WAN bandwidth may have to expand to handle traffic while supporting other emerging applications and business requirements.
- Each courthouse or remote facility should have a high-speed connection back to the State Network unless a high-speed network has been provided by the county already. The speeds will vary for each Circuit depending on bandwidth requirements.
- Throughput on the WAN should be benchmarked at key junctures before the system becomes operational, and should be continually monitored thereafter.
- Since bandwidth provided by the state network is a shared resource, bandwidth management at the circuit level is strongly recommended

### ***References:***

Structural Wiring BICSI Standards

<http://www.bicsi.org/Publications/Index.aspx>

QoS – Quality of Service Guidelines

### ***Wireless Technology***

In the Courts, wireless technology is used for both point-to-point connectivity, as well as multi-point connectivity. Point-to-point is utilized to extend the wide-area network, connecting physically separate networks. Multi-point wireless is used to extend the local area network to wireless users within a limited physical area. It is beneficial to the organization when addressing mobile judicial users within a building, as well as fixed user locations where wired LAN connectivity is unavailable. The following is a list of guidelines that should be considered when developing a wireless security plan.

### ***General Wireless Guidelines***

- Change the default level of product security — out of the box, WLANs implement no security
- Change the out-of-the-box settings — do not use default or null SSIDs or passwords
- Implement wireless access points on switched network ports
- Develop and publish standards and policies for departmental WLANs
- If you are forced to rely on WEP\*, always use 128-bit keys where available
- Implement MAC address tracking to control network security



- Monitor access logs or use network-based intrusion detection to detect unauthorized access or attack
- Highly sensitive networks should use encryption with a minimum of 128 bit, the SSID should not be broadcast, and MAC authentication required

The organization should develop a practical and comprehensive wireless solution, including a detailed security plan, that is based on IEEE 802.1x industry standards and that is supported by the user community.

### ***Multi-point Wireless***

Due to the open nature of wireless, each organization should design and publish security standards for the wireless solution. The wireless LAN (WLAN) industry uses several standards categorized by the IEEE 802.11 classification. This set of standards addresses both bandwidth and security issues. While cost will vary between technologies, the primary consideration should be security through encryption and authentication. Restricted area of coverage for wireless access points should also be considered; covering only the areas within the physically controlled area reduces the accessibility by unauthorized users.

The following is a list of general guidelines that should be considered when developing a wireless security plan and implementing wireless local area networks (WLAN). Because wireless technology enhancements are frequent, current and emerging standards should be consulted during the initial and ongoing planning stages of a multi-point wireless project.

### ***Multi-point Wireless Guidelines***

- Develop and publish standards and policies for departmental WLANs. Address acceptable use and levels of service for multiple user types (if applicable).
- Perform site surveys for wireless coverage, plan ahead for access point locations to address LAN and power requirements.
- Implement wireless access points on switched network ports
- Security must be addressed on two levels: encryption and authentication.
- The newest security standard is 802.11-2007 (sometimes referred to as WPA2), incorporating authentication by 802.1x standard. 802.1x supports authentication server or database service including Remote Authentication Dial-In User Service (RADIUS), LDAP, and Windows domain, and Active Directory. Encryption in 802.11-2007 is strong AES.
- If 802.11-2007 is not used, WPA (WiFi Protected Access) uses stronger encryption than WEP.
- If you are forced to rely on WEP\*, always use 128-bit keys where available. Rotating keys frequently as practical for additional security.
- Change the out-of-the-box settings — do not use default or null SSIDs or passwords. At a minimum, activate the default level of product security.
- Set access point SSID broadcasting to OFF



- Consider implementing VPN with strong encryption for the wireless networks. Place access points outside of the firewall. Use VPN for connectivity to the intranet.
- Implement MAC address authentication and tracking to control network security. Utilize monitoring software to limit network access based on user's physical location and IP address, granting or denying access to services as needed.
- Implement additional authentication if supported by the vendor (RADIUS, LDAP, etc.)
- Monitor access logs or use network-based intrusion detection to detect unauthorized access or attack
- Any public access must be outside the court's network.

### ***Point-to-Point Wireless***

When implementing a wireless solution to connect remote locations, the following items need to be considered:

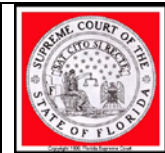
#### ***Point-to-Point Wireless Guidelines***

- Bandwidth / Network Requirements – Video Conferencing, DCR Monitoring, VoIP, data, and latency
- Distance / Path – Line of sight is required.
- Tower Locations and Access
- Security
  - Physical security – Tower location and equipment need to be secure.
  - Network security
- Availability – Recommend 99.98 or better.
- Management – SNMP compliant.
- Warranty and Maintenance – Equipment, tower climbing and maintenance

The organization should develop a practical and comprehensive wireless solution, including a detailed security plan, that is based on IEEE industry standards and that is supported by the user community.

\* Wired Equivalent Privacy (WEP) - The 802.11 standards define WEP as a simple mechanism to protect the over-the-air transmission between WLAN access points and NICs.

Licensed bandwidth has oversight by the FCC, and must adhere to FCC rules and regulations. Licensed bandwidth allows for guaranteed frequency ranges that are assigned to the associated license. This prevents interference with other frequency. Unlicensed bandwidth does not have oversight, and has an associated risk of interference from competing wireless locations. Any interference issues must be negotiated on a case-by-case basis.



### 3.2.2 Security Standards

Information Security should encompass many technical and non-technical areas. This section describes the comprehensive high-level technical security architecture strategy that should be addressed when defining Information Security requirements.

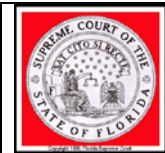
Information Security Standards are organized in four categories:

1. Device Control
2. Personnel Control
3. Network Control
4. Physical Security

These standards address the overarching Information Security needs and provide a framework for developing compliant Information Security Standards and Policies.

#### Device Control

- Access Rights and Privileges - Computer-resident sensitive information shall be protected from unauthorized use, modification, or deletion by the implementation of access control rights and privileges.
- Anti-Virus Protection - Platforms that are susceptible to malicious code shall be equipped with adequate software protection when such protection is available.
- Authentication of Desktop Users - Access to the information devices shall be secured and authenticated using adequate security techniques.
- Backup Policy - Data sensitive devices shall undergo an adequate backup on an adequately periodic basis to protect against loss of information.
- Business Continuity & Disaster Recovery - Formal Business Continuity and Disaster Recovery Plan(s) shall be documented and implemented in accordance with applicable Florida State Courts policy and administrative rules.
- Transmission of Sensitive Data - Sensitive data (security management information, transaction data, passwords and cryptographic keys) shall be exchanged over trusted paths, or using adequate encryption between users, between users and systems, and between systems.
- E-mail Anti-Virus Protection - The entry and exit of viruses and potentially harmful attachments in the email infrastructure shall be effectively limited.
- Platform Level Administration - Local - Local access to system console functions shall be restricted to appropriately authorized Systems Administrator(s).
- Platform Level Administration - Remote – Remote access shall be secured via adequate



authentication.

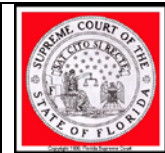
- System Administration Privileges - System administration privileges shall be locally granted by each Covered Entity only to authorized personnel.

### **Personnel Control**

- Acceptable Use Policy – Policy addressing the acceptable use of information technology shall be documented.
- Acceptable Use Training - All employees shall undergo training/briefing/orientation that supports compliance by employees with all elements of acceptable use and applicable Information Security policies and guidelines.
- Dial-Up/Remote Access Policy - Dial-Up and/or Remote Access Policy shall be written and implemented where applicable.
- Sensitive and Exempt Data Handling - All employees with appropriate access shall be trained on handling sensitive and exempt data. FDLE CJIS Guidelines are required for any workstations accessing FCIC/NCIC data directly or through the Judicial Inquiry System (JIS).
- Incident Response - Incident Response procedures shall be maintained which guide response to breaches in device, network, and physical security.

### **Network Control**

- Network - Network security encompasses preventing unauthorized access to the LANs, MAN, and WAN that will be used to access judicial services.
- Device Resistance - All critical devices within the Perimeter Network shall be resistant to attack in relation to known threats for which there are available defenses.
- Network Audit Logs - Network audit logs shall provide sufficient data to support error correction, security breach recovery, and investigation.
- Remote Access - All remote access methods providing access to critical systems shall be identified and inventoried. Remote access to the court's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.
- Wireless Network Security and Management - All wireless networks and devices shall be locally authorized by each Covered Entity and have adequate security configurations.



## Physical Control

- Physical Security Policy – Physical security policies shall adequately address information technology infrastructure.

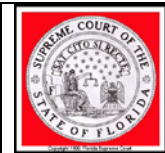
### 3.2.3 System Management Tools

A comprehensive set of management tools will be required to support an integrated information system environment. The system architecture and its components should support centralized monitoring and control. Characteristics of system management include:

- A Systems Management application should be utilized to provide complete systems and network management throughout the enterprise computing environments. Desirable characteristics include Active Directory monitoring, SQL (or equivalent) database monitoring, and detailed and flexible reporting mechanisms.
- Network Management applications should be deployed and integrated to support network management requirements including the hub/switch management and network router. All equipment should be SNMP compliant, and in a Windows environment, WMI compliant. Tools should monitor across VLANs, WANs, and disparate network architectures. Tools should monitor wireless whenever possible. Both IPv4/IPv6 are preferred. Tools should contain the ability to monitor, report, and block offending IP addresses or infected network segments. QoS ability preferred. To work with network management tools, SSH or SSL is preferred over telnet or html. Traffic monitoring systems should utilize a learning mechanism establishing initial baselines that are time corrected and display anomalous traffic with reasonable swiftness. Rules based equipment should allow for frequent base table updating.
- Desktop Management tools should be deployed and integrated to support workstations, software distribution, desktop inventory control and asset tracking of desktop configurations and installed software (metering). Ghost or equivalent imaging software, patch management (such as WSUS), and detailed and flexible reporting mechanisms are recommended.
- Server Management tools should contain the following capabilities:
  - Should be SNMP-compliant
  - Should include the ability to monitor server health including disk, RAM, and process utilization, and whenever possible, power consumption
  - Should support LDAP whenever possible
- Change Control applications should be utilized to help coordinate the activities (such as software code changes, testing and verification of the changes, and related documentation changes) that need to be performed by various organizations.

For all tools, administrators should consider the following:

- For flexibility, look for site or enterprise licensing
- Agent-less tools are not required, but may be preferred
- Reporting/metrics functionality is preferred and strongly recommended



- Email/Text alerts, virus monitoring should be available for all systems, remote management of network, desktops, servers, preferred (provided software meets the established security standards)

It is recommended that a daily health report contain the following information whenever possible:

- SNMP trap information
- Login reports for both successful and failed attempts (wireless, RADIUS, VPN, etc.)
- Switch/router/hub change logs
- Wireless connections
- Server health (average CPU load, RAM and disk utilization, etc.)
- Active Directory additions/deletions/changes
- Restricted traffic attempts and perceived network anomalies

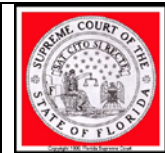
### **3.2.4 Audio and Video Teleconferencing**

The following is a list of recommended guidelines that will serve as a good starting point for defining video conferencing.

#### **Digital Audio and Video Conferencing Standards**

- Must use the TCP/IP network protocol
- Separate VLAN for video
- Standard Definition speed: 384K
- High Definition speed: 768K
- Duplex: Full (512 Units = Half)
- Network speed: 100Mbps (502 Units = 10Mbps)
- Switch and codec: hard-coded speed/duplex
- Video communications must support the H.323 and H.264 SIP multimedia standards
  - H.323 and H.264 standards
  - SIP (must have ability to communicate with H.323 legacy systems) Video conferencing must support H.264 video compression  
Audio conferencing must support G.711 audio compression
- ISDN capability for external connections should adhere to the following standard – H.232/H320 Gateways
- Low Resolution: Based on communications availability. H.323 standard should use a minimum of 256Kbps bandwidth per concurrent video session.
- High Resolution: Minimum of 786kb bandwidth per concurrent video session.
- QoS tag: DSCP AF41
- Ports: 1719, 1720, 3230-3253 TCP/UDP\*

\*PLEASE NOTE – Polycom systems use random port generation while making & receiving video calls. It is recommended that your system be open to port traffic to avoid video signaling problems.



Any endpoint or MCU transversing the internet should be considered best effort with regards to connection, signal quality, and audio/video clarity.

### **3.2.5 Court Reporting Technologies**

Automated court reporting tools have become standard technology in many courtrooms. Use of digital court reporting systems are being standardized and these standards can be reviewed in The Trial Court Performance and Accountability Court Reporting Recommendations for the Provision of Court Reporting Services in Florida's Trial Courts (May 2007). Other court reporting technologies, such as stenographic and real time reporting, are also addressed in this document.

#### ***Other technical considerations:***

- Any remote monitoring and management may require review and planning of bandwidth requirements.
  - Local contingency must be addressed in the event remote communications are interrupted.
  - Bandwidth requirements per remote session (courtroom) should be analyzed and determined before implementation to ensure sufficient bandwidth is available or funding is available. Current standards are 384Kbps or less per DCR session.

#### ***References:***

Technical and Functional Standards for Digital Court Recording (As of October 2008)

Trial Court Performance and Accountability Court Reporting Recommendations for the Provision of Court Reporting Services in Florida's Trial Courts

[http://www.flcourts.org/gen\\_public/court-services/court\\_reporting.shtml#pa](http://www.flcourts.org/gen_public/court-services/court_reporting.shtml#pa)

National Association for Court Management (NACM) "*Making the Verbatim Court Record*"

### **3.2.6 Technical Support**

Define skill sets needed to achieve technology objectives and provide support and maintenance. On call is often required to support 24/7 operations

#### **User Support Ratio**

Minimum service level expectation in the court environment is to provide initial service within the same day as when the call for assistance was received.

Specialized technical services may require dedicated support staff depending on the environment.

Specialized services may include:

- a. Network
- b. Security
- c. Audio Video
- d. ADA



- e. Communications
  - i. Data
  - ii. Voice
- f. Training
- g. Web
  - i. Internet
  - ii. Intranet
- h. Application Development

Other Considerations: Geographic area will impact service levels, and multi-county or large county circuits must consider travel time in service level expectations. Additional staff may be required to meet service level requirements.

Funding for on-going training must be included with staff in order to maintain skill sets required to support the environment.

### **3.2.7 Courtroom Technology Standards**

#### **3.2.7.1 Courtroom – Hearing Room Technology Minimum Requirements**

Courtrooms and hearing rooms need to have the infrastructure in place to deliver information and services to the courtroom. Information is vital whether it is information on a computer screen, a juror's ability to hear the witness, or the ability to setup evidence presentation tools.

As systems with the purpose of providing information to the judge are being developed and becoming available, having a minimum standard for courtroom technology is imperative in order to allow the judge to employ these powerful information delivery tools to make the best most informed decisions possible.

#### ***Standards***

##### Network Devices and Infrastructure

Courtrooms and Hearing Rooms - Network connectivity allows data to flow into the courtroom. At a minimum, there should be network connectivity at the Judge's Bench and Clerk positions in the courtroom to accommodate networked workstations and networked printers. The judge's work station should have a network drop in the hearing room. Additional consideration for network connectivity at the attorney's tables and other areas of the courtroom should be considered. Other networked devices such as Video Conferencing Units would add greater service capability to the courtroom. An analog telephone line in each courtroom and hearing room should be installed to accommodate a full duplex speaker phone as required.



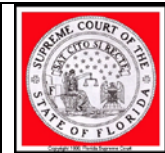
### Task Specific Technology

Courtroom - Sound systems in the courtroom are crucial especially in jury trials where participants must be able to hear all information being presented. In addition, a fixed or portable Assisted Listening Device should be included in any sound system planning. Audio Systems are required to meet ADA requirements.

### Optional

Evidence Presentation - Systems should be able to display a wide range of the many forms of physical and digital evidence used in today's courtrooms. An evidence presentation system should include (but is not limited to) the following support components:

- Display:  
Mobile Display (TV/LCD screen) or Projector:  
A mobile display is recommended only for smaller settings and should support 1920 x 1080 native resolution.  
  
A Projector should support at least 1920 by 1080 native resolution with sufficient brightness for viewing in ambient light (will vary based upon projected image size). + Projector Screen  
  
System should provide audio/video outputs compatible with Courtroom's integrated video displays/audio/DCR system (if applicable)
- Cables:  
Audio/video presentation systems should support prevailing audio/video transmission cable standards such as:  
Analog stereo audio, Composite video, S-video, VGA, S/PDIF, Component, HDMI
- Physical Media:  
Audio/video presentation systems should support prevailing physical media standards such as: CD (R/RW), DVD (+-R/RW), VHS tape, USB storage device (flash or HD), CompactFlash, SD/Smartmedia, Memory Stick
- Digital audio/video standards:  
Audio/video presentation systems should support prevailing digital audio/video standards such as: Audio CD, DVD, VCD, SVCD, WMV, Quicktime, Mpeg4, MP3, OGG,
- Overhead Projector
- Document Camera



### **3.2.7.2 Displays and Presentation**

In many courts the attorneys bring their own presentation equipment or they make arrangements. Some presentation equipment should be available at the courthouse for judges and staff use, as well as for court appointed cases and other contingencies. It is not reasonable to expect attorney's to bring some equipment with them due to bulk and security. The quantity of each item depends on the needs of the individual Circuit Court.

Fixed equipment or portable cart with Video Display and VCR/DVD combo player

This equipment is usually difficult to bring into the courthouse, so they should be available for use in the courtroom. Walls will need to be reinforced and have the proper power outlets and inputs.

Video Camera

Video cameras are often used for child witness testimony and other court events.

Remote Testimony

Courts often have a separate room where a child/individual can be interviewed outside the courtroom. Cameras and microphones are used to bring the interview/testimony into the courtroom.

Projector

Projectors are used for evidence presentation, training, and administrative presentations.

Document Camera

Document cameras are used to present documents on a screen or to present other evidence that needs to be projected.

Portable PA System

Portable audio is critical if the existing sound system needs enhancement due to a large crowd or used in other court areas that are not wired for sound.

Acoustics

There may need to have sound proofing and acoustic panels.

## **3.3 Requirements for Interoperability and Data Exchange Standards**

During the past 30 years, the lack of standards for linking information systems has been responsible for a substantial part of the high costs involved with information exchange and it has contributed significantly to the associated difficulties of exchanging information between agencies. Systems were developed and administered by various agencies for internal priorities, and not necessarily with consideration of the data needs of external entities. Different entities often devoted resources to capture same or similar data. A good example is sentencing data, which must be available to or collected by the judiciary, Clerk of Courts, State Attorney's Office, Public Defender, OSCA, and Departments of Law Enforcement and Corrections. Technological and resource limitations and



reluctance to share data between entities (due to privacy and security issues) have precluded the standardization of data formats and access to data in a fast and user friendly manner.

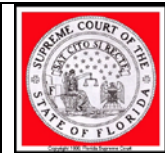
New applications being developed should have web based capabilities for records viewing. Any enhancements or upgrades to existing applications must include support for access through a web browser for viewing of records. To the extent possible, access to add, change, and delete information should migrate towards web based interfaces. Scanning systems and other applications that directly interface with peripherals are difficult to move to web based applications but are possible.

Access to court records and information related to court cases is critical to the court. There are recommended processes that should be undertaken when developing or upgrading applications.

- Utilize a Information System Development Methodology (ISDM) to cover the following:
  - Review business processes and determine if they need to be changed
  - Data modeling
  - Work flow analysis and diagramming
  - Application architecture analysis
  - Strategic planning for application development and maintenance lifecycles
  - Development
  - Documentation
  - Training
  - Testing
  - Implementation
- Utilize a Project Management Methodology specifically designed for use in application development projects.
- Uniform Identifier is used so individuals can be uniquely identified to allow relations to other databases to connect related data (family identifiers are used to tie relationships together is another matter to be resolved). Policy and Operational guidelines/policies have not evolved enough to allow us to collect the information needed for the system to build these relationships in the database i.e. upon arrest collecting the family demographics etc.

The technical standards listed below have been developed across all industry sectors and have the joint backing of many companies (such as Microsoft, Oracle, Sybase, IBM, etc.) that have recognized that information exchange and the resulting gains in productivity and efficiency are at the heart of improved system performance.

- Software applications must support the following standards:
  - Presentation (for Web-based Applications)
    - Standards Compliant XHTML 1.0/HTML 4.01 and later
    - Standards Compliant Cascading Style Sheets 2.1 and later
    - Security - Use industry-proven algorithms, techniques, platform-supplied infrastructure, and vendor-tested and supported technologies.

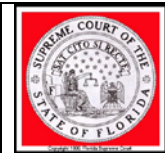


- Application
  - Service Oriented Architecture (SOA) should be applied to applications development processes such as Model–View–Controller (MVC). The presentation layer accesses information via a web service.
  - Where possible, code should be executed on the server (server-side code), not the client.
  - eXtensible Markup Language (XML)
  - Simple Object Access Protocol (SOAP)
  - Web Services AND/OR Representational State Transfer (REST) Web Services
  - American National Standards Institute Structured Query Language (ANSI SQL)
  - W3C ADA/508 Compliance
  - Open Database Connectivity (ODBC), Java Database Connectivity (JDBC), OLEDB, Database Native Clients
  - Remote Procedure Call (RPC)
  - Security
    - Use industry-proven algorithms, techniques, platform-supplied infrastructure, and vendor-tested and supported technologies.
    - Application should handle errors at each layer and should be converted into a user readable language while displaying on the presentation tier. No sensitive security information (including the component name) should be presented on the User Interface.
- Storage
  - American National Standards Institute Structured Query Language (ANSI SQL)
  - Security - Use industry-proven algorithms, techniques, platform-supplied infrastructure, and vendor-tested and supported technologies.

### **3.3.1 Data Exchange Standards (eXtensible Markup Language (XML))**

The current data exchange methodologies and application program interfaces (APIs) need to be investigated and defined for the applications that will comprise the judicial application. The applications' API definitions should include their availability to other operating systems and programming languages. Further, they should include function calls, data types, and any special considerations regarding accessing the application services.

Extensible Markup Language (XML) should be explored as the primary method for information exchange within an integrated judicial system. eXtensible Markup Language (XML) defines a standard format that allows document content to be stored, exchanged, displayed, and processed. Data is described in terms of meaningful pieces of information (title, author, date of preparation, order number, address etc.) that can be used across applications and computer systems for many



different purposes. The most notable and widely adopted work in the development of XML standards is the World Wide Web Consortium (W3C), which has the objective of building open (non-proprietary) technology. The courts also recognize the ECF 4.0 standards for XML standards in the judicial/legal environment.

There are three popular trends which should be used as a basis for building new standards unique to the judicial environment.

- The use of XML schemas to reflect the definition of data types.
- The use of emerging XML protocols for defining the envelope for interchange.
- The use of web services as a model for integrating systems.

### **3.3.1.1 Principles and Procedures for Development of XML Specifications for an Integrated Judicial System**

The diverse requirements of data exchange between the key agencies (such as FDLE, Highway Safety, and Department of Corrections), judicial locations, and the Office of the State Courts Administrator (OSCA) can be accomplished using XML technology. The recommended principles and procedures for development of XML specifications for the judicial application are included below.

#### **Principles**

- Any XML specification developed should be guided by the principles put forth by the World Wide Web Consortium (W3C) and ECF 4.0.
- XML specifications shall be over-inclusive by specifying those elements that may be required by fewer than all participants and making those elements optional.
- It is the responsibility of each judicial/county/circuit location to ensure that all system-specific features are removed prior to transmission to another group.
- Wherever possible, previously developed standards and specifications should be adopted or extended.
- XML specifications shall be broad enough to accommodate jurisdictional differences.
- When operational requirements dictate differences in specificity, mapping from the more specific elements to the less specific elements shall be made available.
- Data elements may contain other elements and may even be recursive.
- Certain complex elements are sufficiently independent and driven by group business rules such that they cannot be used by more than one organization. In such cases, the shareable simple elements contained within the complex element are defined.
- For every element, a default minimum attribute set will be available for use. These attribute(s) will, for the most part, be optional.
- Data element content length generally will not be restricted in the court's Data Element Dictionary developed by previous JAD sessions for that particular application. However, there may be some elements for which a maxLength parameter is specified due to constraints of existing, prevailing statewide systems (such as OBTS). Further, specific



implementations can incorporate maxLength-type parameters for other elements into their schema for validation purposes.

- Generic tag names within complex elements are preferred when the data is clearly the same entity (e.g., <state> may be used to refer to both the state of the postal address and the state of vehicle registration). Generic tag names should be avoided when the meaning is ambiguous (e.g., <number> should not be used to represent both a phone number and an operator license number; explicit tag names should be used).

### **Procedures**

The process and procedures to be used by the courts to achieve success in bringing the aforementioned specifications closer to interoperability are:

- Identify each participant's requirements and goals. Ensure all participants have at least a moderate understanding of each other's needs.
- Identify similar information being shared by participants, and the differences and similarities between tag names.
- Identify and resolve non-substantive differences (e.g., tag capitalization, naming conventions).
- Identify and resolve those substantive differences that can be resolved quickly. (e.g., tag names for person name elements).
- Identify those substantive differences that are difficult to resolve. Where possible, resolve them. Where resolution is not possible, usually due to differing requirements, ensure that there is no tag-name overlap and document the differences.
- Develop a plan for problem resolution and implementation (with tasks, goals, and objectives) to be accomplished over a defined schedule.

### **3.3.2 Database Standards**

Database connectivity to some databases may not be possible due to database driver restrictions or network restrictions at the location. For each participating agency/entity, a plan should be cooperatively developed on how to connect to, access, and format the data maintained in the particular database source. These databases should be:

- Relational
- ANSI SQL
- Package ODBC and/or JDBC drivers with the database platform
- Secured - Use industry-proven algorithms, techniques, platform-supplied infrastructure, and vendor-tested and supported technologies.
- Backed up and have transaction logs running for recovery to point in time failures.
- Have a tested recovery plan.



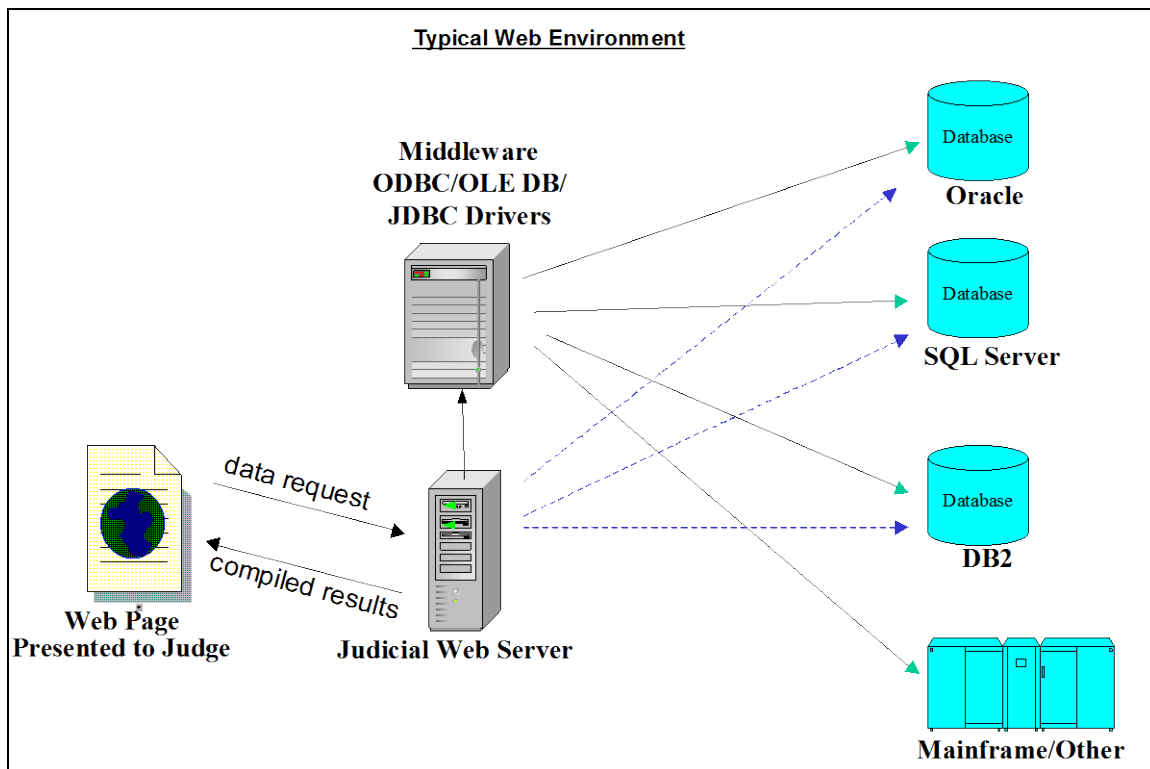
### 3.3.3 Database Connectivity

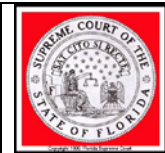
A detailed system architecture should be defined that will meet the business requirements of the judicial application. The system architecture should describe the structure and organization of the information systems supporting specific circuit/county/judicial location functions, and provide the technical system specifications based on the functional requirements. It should describe the complete set of system and network infrastructure components that are installed or planned for installation. It should also include an approach to information sharing (database connectivity) and workflow coordination between business functions, external sources, and users of business information. Also, the architecture should define recommended drivers/middleware once the database and application development software for the system are finalized.

The communication technologies (database drivers) needed to allow transmittal and sharing of access to and utilization of information for various databases in the circuits may include:

- Open Database Connectivity (ODBC)
- Object Linking and Embedding (OLE DB) and/or
- Java Database Connectivity (JDBC)

Figure 6. Conceptual Data Exchange Environment





## 3.4 Cloud Computing

Cloud computing has the potential to greatly reduce waste, increase data center efficiency and utilization rates, and lower operating costs. Using the power of technology to improve performance and lower the cost of government operations. Cloud computing is an approach to delivering IT services that promises to be highly agile and lower costs, especially up-front costs. This approach not only impacts the way computing is used, but also the technology and processes that are used to construct and manage IT within enterprises and service providers. Technologies like cloud computing and virtualization are rapidly being adopted by enterprise IT managers to better deliver services to their customers, lower IT costs and improve operational efficiencies. Cloud computing is primarily a business decision of operating expense vs. capital expense.

### 3.4.1 Definition of Cloud Computing

As defined by the National Institute of Standards and Technology (NIST)<sup>1</sup>, cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of essential characteristics, deployment models, and various service models.

### 3.4.2 Characteristics of the Cloud

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale up and rapidly released to quickly scale down. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured Service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can

<sup>1</sup> <http://csrc.nist.gov/groups/SNS/cloud-computing/>.



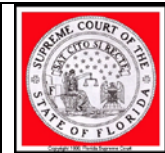
be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

### 3.4.3 Deployment Models

- **Private cloud.** The cloud infrastructure is operated solely for one organization. It may be managed by the organization or a third party and may exist on or off premises.
- **Community cloud.** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organization or a third party and may exist on or off premises.
- **Public cloud.** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. Any selected public cloud computing solution shall be configured, deployed, and managed to meet the judicial branch's security, privacy, and other requirements. Court data must be protected in a manner consistent with judicial branch's policies.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

### 3.4.4 Service Models

- **Cloud Software as a Service (SaaS).** Provides the consumer the ability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based e-mail). Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **Cloud Platform as a Service (PaaS).** Provides the consumer the ability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. Its main purpose is to reduce the cost and complexity of purchasing, housing, and managing the underlying hardware and software components of the platform. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- **Cloud Infrastructure as a Service (IaaS).** Provides the consumer the ability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as



virtualized objects controllable via a service interface. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

### **3.4.5 Data Protection**

Data must be kept secure while at rest, in transit, and in use. Access controls shall be in place to keep data away from unauthorized users.

Data must be sanitized when a storage device is removed from service or moved elsewhere to be stored. Data sanitization also applies to backup copies made for recovery and restoration of service, and also residual data remaining upon termination of service.

### **3.4.6 Service Level Agreement (SLA)**

A SLA between the Court and the cloud provider shall detail the expected level of service to be delivered, such as licensing of services, criteria for acceptable use, service suspension and termination, limitations on liability, privacy policy, and modifications to the terms of service.

### **3.4.7 Standards Development**

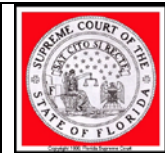
As we move to the cloud, we must be vigilant in our efforts to ensure the standards are in place for a cloud computing environment. As part of the Federal Cloud Computing Initiative, the National Institute of Standards and Technology (NIST)<sup>2</sup> is leading and facilitating the development of cloud computing standards which respond to high priority security, interoperability, and portability requirements.

Current cloud computing standards development activities, conducted by the NIST Information Technology Laboratory (ITL), include:

- **Special Publications:** In 2009, NIST made the widely adopted and referenced NIST Definition of Cloud Computing publicly available. NIST is in the process of developing a series of Special Publications (SP) related to cloud computing.
- **Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC):** The SAJAAC goal is to facilitate the development of cloud computing standards. SAJACC will include a publicly accessible NIST hosted portal which facilitates the exchange of verifiable information regarding the extent to which pre-standard candidate interface specifications satisfy key cloud computing requirements. The expectation is that SAJACC will help to

---

<sup>2</sup> National Institute of Standards and Technology, "Summary of NIST Cloud Computing Standards Development Efforts" (government document, 2010).

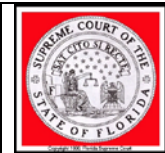


accelerate the development of cloud computing standards and, as a bi-product of its information dissemination function, increase the level of confidence to enable cloud computing adoption.

- **Federal Risk and Authorization Management Program (FedRAMP):** NIST's role is to support the definition of a consistent technical process that will be used by FedRAMP to assess the security posture of specific cloud service implementations. NIST serves as a technical advisor for the FedRAMP process that will be implemented by the Federal CIO Council.

#### **Title 44 of the United States Code:**

**Federal Information Security Management Act Certification ("FISMA", [44 U.S.C. § 3541](#), *et seq.*):** FISMA is a [United States federal law](#) enacted in 2002 as Title III of the [E-Government Act of 2002](#) (Pub.L. 107-347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide [information security](#) for the information and [information systems](#) that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.



## Appendix

### Benefits of Cloud Computing

There was a time when every household, town, farm or village had its own water well. Today, shared public utilities give us access to clean water by simply turning on the tap; cloud computing works in a similar fashion. Just like the water from the tap in our kitchen, cloud computing services can be turned on or off quickly as needed. Like at the water company, there is a team of dedicated professionals making sure the service provided is safe and available on a 24/7 basis. Best of all, in addition to saving water when the tap is not on, we are saving money by not paying for resources we do not currently need.

- **Economical.** Cloud computing is a pay-as-you-go approach to IT, in which a low initial investment is required at the onset. Additional investment is incurred as system use increases and costs can decrease if usage decreases. In this way, cash flow is equivalent to total system cost.
- **Flexible.** IT departments that anticipate fluctuations in user load do not have to scramble to secure additional hardware and software. With cloud computing, they can add and subtract capacity as network load dictates, and pay only for what is used.
- **Rapid Implementation.** Without the need to go through the procurement and certification processes, and with a near-limitless selection of services, tools, and features, cloud computing helps projects commence in record time.
- **Consistent Service.** Network outages can send an IT department scrambling for answers. Cloud computing can offer a higher level of service and reliability, and an immediate response to emergency situations.
- **Increased Effectiveness.** Cloud computing frees the user from the finer details of IT system configuration and maintenance, enabling them to spend more time on mission-critical tasks and less time on IT operations and maintenance.
- **Energy Efficient.** Because resources are pooled, each user community does not need to have its own dedicated IT infrastructure. Several groups can share computing resources, leading to higher utilization rates, fewer servers, and less energy consumption.
- **Price transparency will drive email costs down.** One of the major benefits of cloud-based email is that the costs become extremely public and visible. Google has already set a price floor and Microsoft has undercut its channel. This cost transparency will elevate the competition on price which will drive costs down.
- **Cloud delivery will increase the value and pervasiveness of email.** In a surprising and counterintuitive effect, we believe that cloud delivery will make email the go-to tool for even more situations than today. Consider if our email is available from any device, anywhere, anytime, then why wouldn't we use it? Especially if the alternatives of accessing a wiki or firing up an instant messaging client are not available so conveniently.



- ***Cloud delivery will help make mobile email ubiquitous among information workers.***  
It is clear why today only mobile executives get BlackBerry or Windows Mobile devices. Mobile email is expensive. It cost approximately \$10 per user per month for BlackBerry device support. With the increase in competition from Microsoft, Google, Cisco, and innovative providers like Synchronica, this cost will inevitably decrease and make it possible to deliver basic mobile email to the masses at a much lower cost.

## **Utilizing Cloud**

“The cloud” is not another industry buzz word, but a broad category which will drive the next phase of the Courts projects. For IT and business managers already inundated with information about the promise of a cloud centric infrastructure, the question is not whether to use the cloud, but how. Public cloud environments are not as well known, therefore, it is difficult to infer the impact of moving particular applications to the public cloud without actually testing.

### **Understand your own environment.**

In addition to knowing what applications the Courts would like to move to the cloud, IT managers need a deep understanding of how applications perform across the WAN today, as well as which users are most dependent on particular applications. IT managers need to proactively aggregate information based on geography, applications, and individual users. They have to be ready to quickly assess, discover, and eliminate network-related problems in order to support consolidated cloud environments. Ideally managers should be equipped to aggregate this information without requiring more distributed hardware that goes against the grain of consolidation initiatives.

### **Optimize what you already have and expect the same performance from a cloud provider.**

Courts already use WAN optimization either across their organization and/or in key locations in order to accelerate end-user computing and collaboration, disaster recovery operations, and cut bandwidth needs. Organizations now need to leverage WAN optimization across the board to prepare all business locations for a more distributed world. At the same time Courts considers cloud service providers and WAN optimization solutions, it is imperative to confirm that the two map to each other. Your WAN optimization provider should have a form-factor (usually a virtual appliance) that will easily slot into a public cloud computing environment or a private cloud implementation. Furthermore, your cloud service provider should be one who embraces the fact that performance-enhancing products like WAN optimization are necessary to make their cloud worthy of production use in enterprises.

### **Consolidate to the core and at the edge.**

Make certain you have a good plan to discover all of the applications and servers in your environment and which ones can effectively be consolidated today. Such a plan will allow you to quickly map the applications or services that could potentially be moved to a public cloud, as well as which services must remain distributed. Use branch-office in-a-box technologies for services that must remain distributed. These technologies extend many cloud benefits, such as simplified



management and virtualization all the way to the edge of your network enabling you to drive cost efficiency from the core to the edge of your IT operations.

