Supreme Court of Florida
Office of the State Courts Administrator

Integration and Interoperability Document

Version 2.4

19 April 2016

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
05/05/2011	2.1	Lakisha Hall	Updated Desktop Standards section as a result of the FCTC May 4, 2011 meeting
10/15/2013	2.2	Technical Standards Subcommittee	Updated entire document
05/09/2014	2.3	Technical Standards Subcommittee	Added new section 3.3.1.2 Data Transmission
04/19/2016	2.4	Technical Standards Subcommittee	Updated entire document

Table of Contents

Figures

1. Overview

This section contains subsections that describe the scope of the processes to which the Integration and Interoperability 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 strategic vision of the Florida Courts Technology Commission relative to integration and interoperability among heterogeneous systems.

3. Requirements and Standards for Integration & Interoperability

This section contains the preliminary requirements and recommended standards for interoperability and integration between technology systems that provide information to or on behalf of the judicial branch. The requirements and standards were defined by analyzing Legislative/Supreme Court mandates, functional requirements, existing information systems architecture, and infrastructure reports, and incorporating the results of that analysis into a solution that leverages contemporary information technology management industry standards and best practices for optimal performance, return on investment and efficient technical solutions.

3.1 Diagrams

The diagrams in this section give an overview of the conceptual network architecture for the courts (Figure 1), for the circuits (Figure 2) and court/clerk approved interface method (Figure 3).

Figure 1. Florida Courts Conceptual Network Design

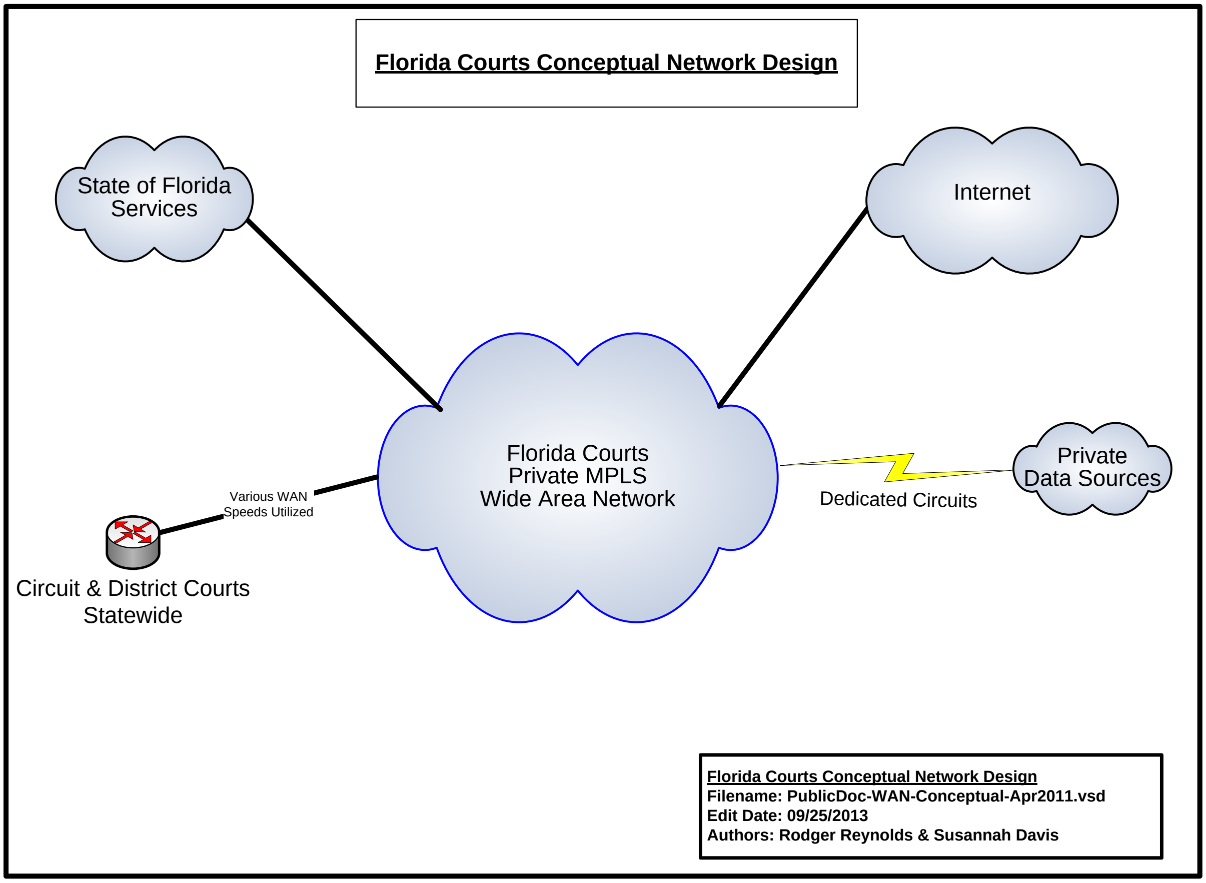

Florida Courts Conceptual Network Design
State of Florida Services
Internet
Florida Courts Private MPLS Wide Area Network
Various WAN Speeds Utilized
Circuit & District Courts Statewide
Dedicated Circuits
Private Data Sources
Florida Courts Conceptual Network Design
Filename: PublicDoc-WAN-Conceptual-Apr2011.vsd
Edit Date: 09/25/2013
Authors: Rodger Reynolds & Susannah Davis

Figure 2. Florida Courts Conceptual Circuit Network Design

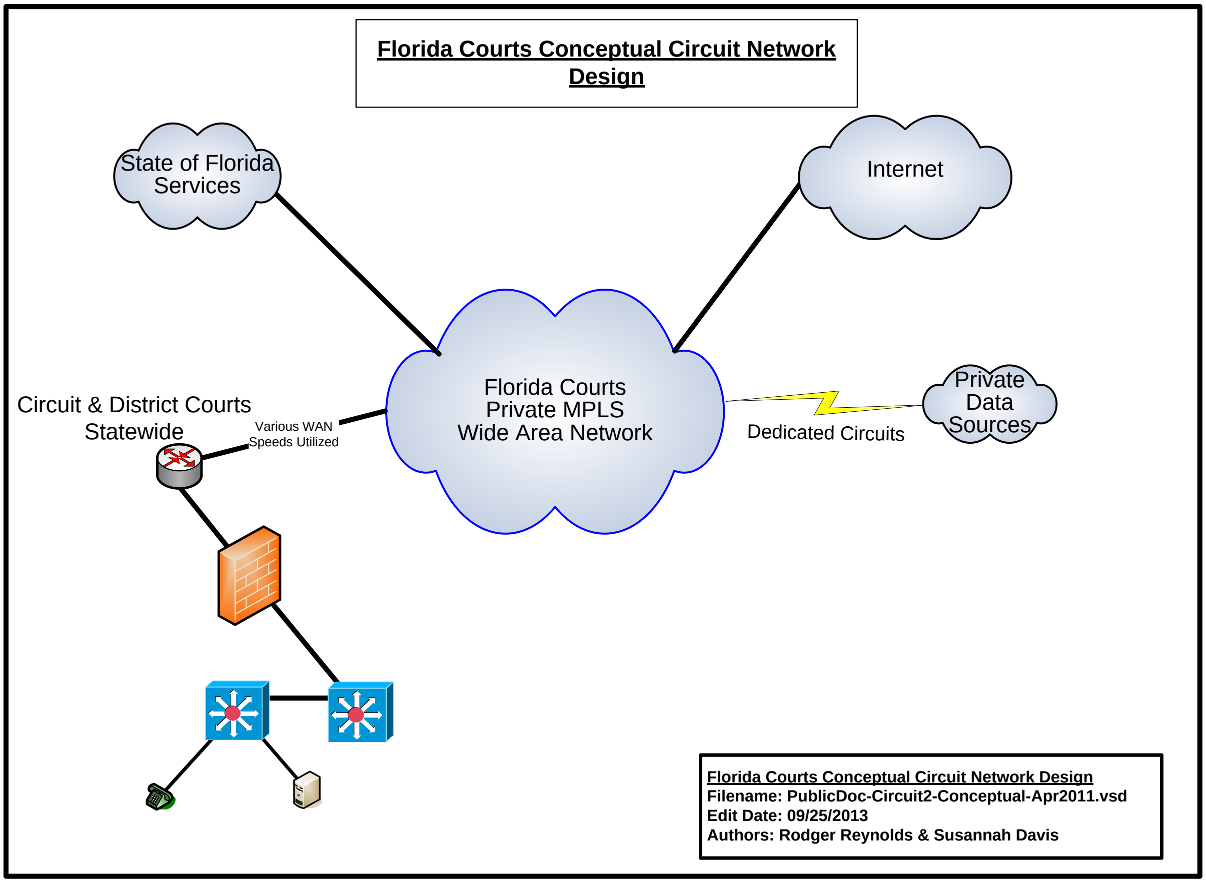
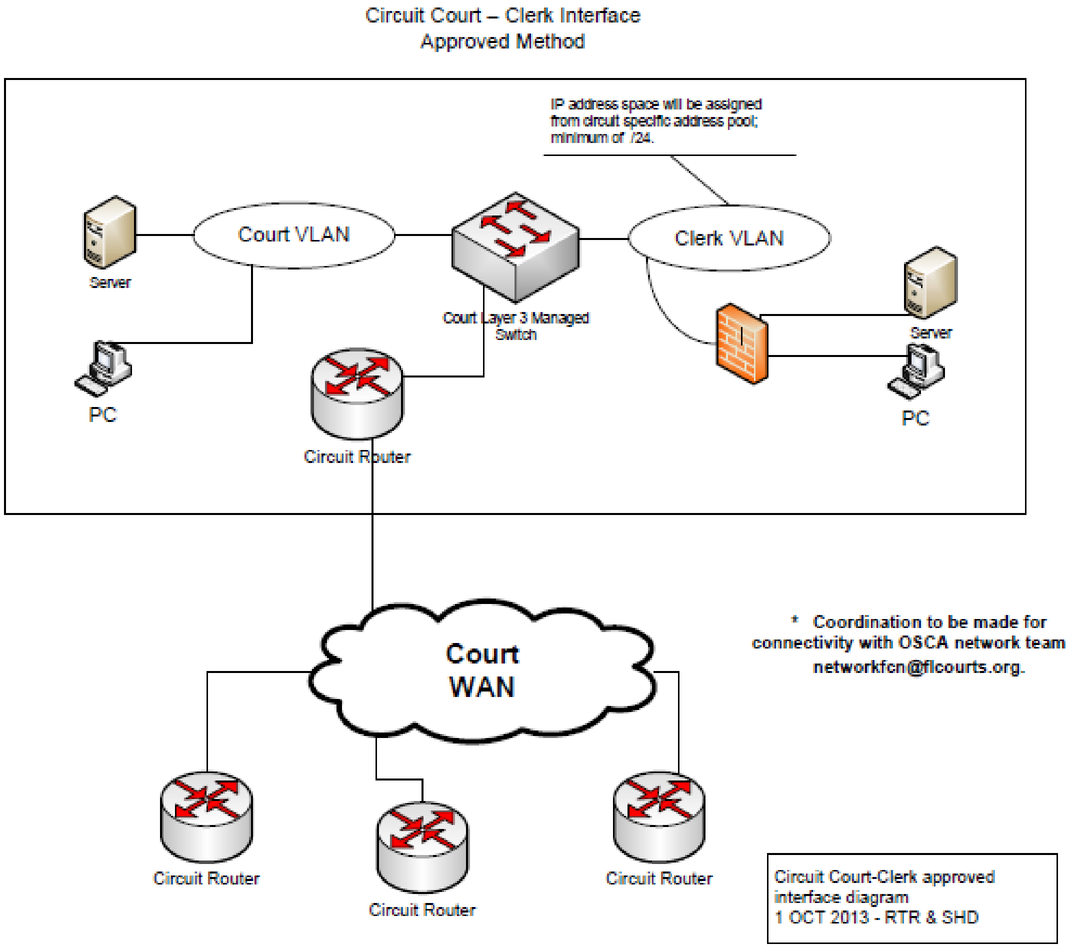

Florida Courts Conceptual Circuit Network Design
State of Florida Services
Internet
Florida Courts Private MPLS Wide Area Network
Circuit & District Courts Statewide
Various WAN Speeds Utilized
Dedicated Circuits
Private Data Sources
Florida Courts Conceptual Circuit Network Design
Filename: PublicDoc-Circuit2-Conceptual-Apr2011.vsd
Edit Date: 09/25/2013
Authors: Rodger Reynolds & Susannah Davis

Figure 3. Circuit Court – Clerk Interface Approved Method


Circuit Court – Clerk Interface
Approved Method
IP address space will be assigned from circuit specific address pool; minimum of /24.
Server
Court VLAN
Court Layer 3 Managed Switch
Clerk VLAN
Server
PC
Circuit Router
PC
Court WAN
Circuit Router
Circuit Router
Circuit Router

* Coordination to be made for connectivity with OSCA network team at networkfcn@flcourts.org.

Circuit Court-Clerk approved interface diagram
1 OCT 2013 - RTR & SHD

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 a strategic approach to hardware and software standardization and life cycle management that will assist circuits in the planning, procuring and implementation of technologies necessary to comply with Supreme Court and Legislative Technology Mandates. Florida Statue 29.008 states that counties within each Judicial Circuit are responsible to fund the court's technology needs, including but not limited to computer hardware (e.g., PCs, video displays, laptops, servers, etc.). To most effectively manage the technology's total cost of ownership, life cycle management should include hardware and software procurement strategies, physical asset management, technical support strategies, and retirement and disposal strategies that maximize the hardware's utility in support of the court's business objectives. Finally, when planning technology solutions, it is imperative to remember that the personnel costs requisite for the maintenance of the solutions often exceed the cost of the physical solution itself. Proper support ratios should be factored in to ensure the efficacy of the solution.

The goal of these guidelines is twofold: first, provide a blueprint for a robust, extensible infrastructure that will support the growth, integration and interoperability of information systems supporting the judicial branch; and secondly, reduce aggregate costs through standards that offer economies of scale.

3.2.1.1 Desktop PC Standards

Desktop Personal Computer ("PC") procurements must be scheduled to meet certain life cycle and performance objectives. Due to increasingly intensive software requirements, a three year life cycle is recommended. The minimum and recommended performance level requirements for desktops currently are listed in Figures 4 and 5. The performance level required will be determined by evaluating system needs, including the number, type and complexity of applications being run; system resources necessary to simultaneously run these applications; and performance metrics requisite for compliance with court standards.

Courtroom/Hearing Room

Video displays: Per the Court Application Processing System ("CAPS") standards, courtroom and hearing room displays shall have sufficient screen size to display multiple electronic documents. The minimum recommended size for a video display is 30". Video display installations should allow for a range of movement and flexible placement so as to prevent obstruction of the judge's view of the courtroom or hearing room. Due to the diverse size, complexity and nature of myriad judicial proceedings, the final determination for size and placement may vary depending on the environment.

Judge’s Chambers

Video display: 22” or greater with capability for dual displays.

Video displays

Video display replacement lifecycles may differ from desktop lifecycles based on functionality and usage requirements. Touch screen displays shall be used where deemed appropriate by the court.

Figure 4. Minimum Desktop Configurations for New Machines

		Details
Hardware	**Processor**	Dual Core Business Class Intel or AMD (3.4 GHz or greater)
	Memory (RAM)	8 GB or greater
	Storage	500 GB Solid State Drives (“SSD”)
	Video	DirectX 9 or greater capable (WDDM Driver Support recommended)
	Graphics RAM	256 MB or greater, system should be able to accommodate dual displays
	Sound	Audio is required in accordance with planned use of the system
	Ports	HDMI & multiple USB 3.0 ports as required
	Optical	DVD-RW combo drive
	Life Cycle	3 Years
Network Connectivity	**Bandwidth**	100/1000BaseT Ethernet, wireless as required

3.2.1.2 Laptop Standards

The court’s migration toward a paperless environment and the implementation of electronic warrant applications offers unprecedented access to judicial officers in nontraditional venues and create an increased need for access to electronic court files/forms from secure, mobile devices.

Figure 5. Recommended Laptop Configurations

		Details
Hardware	**Processor**	Dual Core Business Class Intel or AMD (3 GHz or greater)
	Memory (RAM)	8GB or greater

	Storage	250 GB Solid State Drives ("SSD")
	Graphics	DirectX 9 or greater Capable (WDDM Driver Support recommended) 256 MB (in addition to RAM)
	Sound	Audio required
	Ports	HDMI or mini-display port & multiple USB 3.0 ports as required
	Optical	DVD-RW drive (internal or external as needed)
	Lifecycle	3 years
Network Connectivity	**Bandwidth**	Integrated 100/1000 Ethernet LAN (standard)
	Wireless	Internal adapter supporting 802.11 b/g/n/ac

3.2.1.3 Client (Desktop/laptop) Software Standards

Software requirements for desktops provide a standardized environment for users. This standardization will both simplify and increase the efficiency of the initial software deployment and on-going support for desktops and laptops.

Figure 6. Software Requirements and Standards

Software	Details
Operating System	Windows 7 Professional or higher (OS must be active in the MS Support Life Cycle for patches and updates)
Office Suite	Microsoft Office 2010 or greater or compatible format
HTML Browser	Microsoft Internet Explorer 10 or higher
Other Applications	1) PDF Reader 2) Anti-virus

3.2.1.4 Mobile Devices

This document defines mobile devices for as those that have sufficient computing power for Internet access, email reception, client side applications and interoperability with server side applications. Examples of these mobile personal computing devices include but are not limited to tablets, smart phones, and hybrids. Mobile devices with limited security features should be limited to less sensitive areas of access unless a specialized security measure can be applied that will meet security standards. Mobile device usage must comply with the Criminal Justice Information Services (CJIS) Security Policy under the U.S. Department of Justice, Federal Bureau of Investigation.

3.2.1.5 Recommended Mobile Device Configurations

All mobile devices should exceed minimum standards available at time of purchase.

3.2.1.6 Mobile Device Computing: Any device, anytime, anywhere

Mobile computing technologies increase productivity and flexibility, as well as support continuity of operations in an emergency. Mobile Computing is a rapidly growing segment of court technology; however, with new efficiencies come new security risks: great diligence must be applied to ensure that developing standards for e-filing and data protection factor devices that can access, view, manipulate and store private court information.

Mobile devices generally refer to smartphones and tablet devices that support multiple wireless network connectivity options (primarily cellular and Wi-Fi as well as voice and data applications. This section will focus on the mobile computing, or data element.

Mobile Device Management (MDM)
A key component to successful control and administration of mobile computing is a Mobile Device Management (MDM) Enterprise System that provides security, accessibility and content policies on many popular tablets and smart phones.

MDM products have been developed to mitigate threats to mobile devices by enabling enterprise-controlled device configuration, security policy enforcement, compliance monitoring, and management (e.g., remotely lock and/or wipe a mobile device that has been reported as lost or stolen). MDM solutions typically include an enterprise server(s) component and an application installed on the mobile device to manage device configuration and security and report device status to the MDM.

Small Florida court technology budgets juxtaposed against the tremendous popularity of the smartphone and tablet have led to an unprecedented rise in Bring Your Own Device, or BYOD. Standards to exercise control, manage expectations, and define acceptable use policies should be developed and implemented for all such users.

DDNA
Securing mobile devices should focus on the following 4 categories:

- **Device** security: methods to prevent unauthorized device use, such as an MDM.
- **Data** security: protecting data at rest even on lost/stolen device, such as an MDM.
- **Network** security: network protocols and encryption of data in transmission.
- **Application** security: security of the applications, and operating system, such as a Mobile Application Management MAM.

Recommended MDM Requirements

- Enforce passcodes on devices.
- Allow remote location of device.
- Allow remote wiping of device’s drive/data.
- Allow remote locking.
- Detect rooted/jailbroken phones, which are more vulnerable to malicious code.
- Inventory of devices.
- Policy compliance.

Mobile Application Management (MAM)

Mobile application management (MAM) allows the court to set up an enterprise application store to deploy approved applications, to enforce application policies, and remotely upgrade or uninstall applications.

To mitigate the threat of malicious or vulnerable mobile applications to mobile devices, the court should use MAM to provision for application whitelisting, or allowing installation of mobile applications from authorized enterprise application stores application blacklisting, which blocks the installation of known vulnerable applications.

Recommended MAM Requirements

- Allow for the installation of applications from a private site.
- Control the push/pull of updates to devices.
- Allow for the remote installation of applications.
- Allow for the remote wiping of non–standard applications.
- Whitelisting of select applications from public sites.
- Blacklisting of select applications based either on application or site.
- Application Inventory.

Standards for Acceptable Use: Managing Expectations

Until such time as the Florida Court Technology Commission approves a standard policy, each circuit is recommended to develop an acceptable use consent policy that will outline expectations for security, support and data access on a mobile device. It is recommended that each circuit develop a policy for approval by the Chief Judge. This policy should at a minimum address the following areas:

- What is the circuit policy for bring your own device (BYOD) hardware?
- For BYOD devices:
    - What is the data backup policy?
    - What is the extent of policy enforcement versus device support?
        - Security enforcement-when can a device be wiped?
    - Is the user cognizant of rules that constitute the creation of public records?

  - What enforcement exists for connectivity to unsecured networks (e.g., public wireless connection)
  - Is confidential data storage on the device prohibited?
- For court provided devices:
  - What are acceptable recreational uses for the device (music, photos)?
  - What is the data backup policy?
  - Are secure network connections enforced?
  - What is the acceptable use of data storage on private or public cloud?

Wireless Networking Security

Though both wired and wireless networks are vulnerable to the threat that intruders might snoop out network traffic, or inject rogue traffic, wireless networks are clearly more susceptible to data theft and hijack. Mobile computing poses an inherent risk to data security that must be strictly managed and monitored. Using a VPN tunnel to encrypt mobile access to corporate resources makes for an excellent first line of defense. Additionally, it is important to educate users concerning the dangers of connecting to a wireless network that does not use 256 bit WPA2 encryption.

Users should understand that most public Wi-Fi is not encrypted and is, by its nature, not secure. By utilizing an encrypted VPN connection, the data transmitted between the device and the VPN endpoint are encrypted, even though the Wi-Fi connection itself is not encrypted. If no VPN is in use, then using encrypted protocols (such as HTTPS instead of HTTP) where possible will provide encryption between the device and the remote endpoint.

For internal wireless court/county networks, VLANS or MAC address filtering provide additional controls over secure connectivity.

Bluetooth settings, when not in use, should be turned off.

Best Practices for Criminal Justice Information Systems Connections

Only use properly encrypted connections.

Best Practices for Non-CJIS Connections

For wireless connections, only use properly encrypted connections. There is other potential confidential or sensitive data transmitted outside of CJIS systems.

Be aware of Federal Information Processing Standards (FIPS) 71A-1 Subsections 001-023, and the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security Policy Sections 4.3, Personally Identifiable Information, and Section 5 regarding securing technology that accesses, stores, transmits, and logs Criminal Justice Information governed by this referenced policy. The most current version of this policy can be viewed at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/.

3.2.1.7 Servers

Production servers should support both common/shared services as well as organization-specific services. 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.

3.2.1.8 Network Components

Courts Local Area Network (“LAN”)

Considerations/Recommendations

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

- Naming conventions using Domain Name Service (“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.
    - Switches shall be manageable via IP or other remote protocol.
- Scalable high speed Ethernet/Fiber switches.
- Bandwidth standards and requirements within and among each judicial location are recommended at:
    - Gigabit to servers.
    - Gigabit to workstations.

Use of existing LAN technology at the judicial locations should be evaluated on a location-by-location basis. Where required, the LAN infrastructure should be upgraded to meet the standard.

Any LAN technology dedicated for use by the court should meet 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 *wire-speed* 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).
Software	Intelligent services: Layer 3 routing support via RIP, OSPF, static IP routing. Dynamic IP unicast routing, smart multicast routing, routed access control lists (ACLs), Hot Standby Router Protocol (HSRP) support and Virtual Router Redundancy Protocol (VRRP).

Courts Wide Area Network ("WAN")

The WAN infrastructure supporting the courts will use the State network as its primary transport media. Specific WAN hardware and software solutions should be evaluated and customized to handle the additional traffic that may be required from the system. Integration of local county network infrastructure to the State Network will be addressed on a case-by-case basis in compliance with definitions set forth in Florida Statue 29.008(f)(2).

Considerations/Recommendations

- The courts should strive to standardize DNS 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 are compliant with 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 already been provided by the county. Network speeds for each circuit will vary depending on bandwidth requirements.
- Throughput on the WAN should be benchmarked at key junctures before the system becomes operational, and monitored continually thereafter.
- State-provided bandwidth is a shared resource; accordingly, bandwidth management at the circuit level is strongly recommended.

Wireless Technologies

Wi-Fi

In the courts, wireless technologies include point-to-point connectivity and multi-point connectivity ("Wi-Fi"). Point-to-point is utilized to extend a WAN, connecting physically separate networks. Multi-point wireless is used to extend the LAN to wireless users within a limited geographic area. Wi-Fi is beneficial when providing network connectivity for mobile judicial users, as well as fixed-user locations where wired LAN connectivity is unavailable. The following guidelines 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.
- At a minimum use 128-bit keys or greater 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.
- Disable WPS (Wi-Fi Protected Setup).

- Must meet current CJIS security standards.

Each circuit should develop a practical and comprehensive wireless solution including a detailed IEEE 802.1x –based security plan.

Multi-Point Wireless

Due to the open broadcast nature of wireless networks, each organization should design and publish security standards for their wireless solution. Wireless LAN (“WLAN”) industry uses several standards defined by the IEEE 802.11 classification that addresses both bandwidth and security issues. While cost will vary between technologies, priority for essential elements such as security through encryption and authentication is strongly recommended. Restricting the 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 general guidelines should be considered when developing a wireless security plan and implementing WLAN. Given the ongoing evolution of wireless standards, any guidelines and metrics should be reviewed during the planning stages of any multi-point wireless project.

Multi-Point Wireless Guidelines

- Develop and publish standards and policies for departmental WLANs, including acceptable use and levels of service for multiple user types (if applicable).
- Perform site surveys for wireless coverage, planning ahead for access point locations to address LAN and power requirements.
- Implement wireless access points on switched network ports.
- Address security 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.
- WPA (Wi-Fi Protected Access) will be used as the minimum.
- 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 attacks.
- All publicly accessible Wi-Fi must be outside the court's internal 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, Digital Court Recording ("DCR") Monitoring, VoIP, data volume, 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: –Uptime percentage of 99.98 or better is recommended.
- Management: Utilities should be Simple Network Management Protocol ("SNMP") compliant.
- Warranty and Maintenance: Equipment, tower climbing and maintenance should be included.

Each circuit should develop a practical and comprehensive wireless solution including a detailed IEEE 802.1x –based security plan.

Licensed bandwidth has oversight by the Federal Communications Commission ("FCC"), and must adhere to FCC rules and regulations. Licensed bandwidth guarantees frequency ranges that are assigned to the associated license, preventing interference with other frequencies. Unlicensed bandwidth is not under FCC oversight, and carries the 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 encompasses 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:

- Device Control
- Personnel Control

- Network Control
- Physical Security

These standards address the overarching Information Security needs and provide a framework for developing compliant Information Security Standards and Policies. Security Standards shall comply with CJIS Security Policy under the U.S. Department of Justice, Federal Bureau of Investigation where applicable.

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: Desktop access shall be secured and authenticated using adequate security techniques.

- Backup Policy: Data storage devices shall undergo sufficient periodic backup 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 using adequate encryption between users, between users and systems, or between systems.

- E-mail Anti-Virus Protection: Proactive installation and management of software/hardware to safeguard against the injection of malware, viruses or other code via email or email attachments is required.

- Platform Level Administration (Local): Local access to system console functions shall be restricted to appropriately authorized personnel.

- Platform Level Administration (Remote): Remote access shall be secured via adequate authentication and restricted to appropriately authorized personnel.

- System Administration Privileges: System administration privileges shall be locally granted only to appropriately authorized personnel.

Personnel Control

- Acceptable Use Policy: Policies addressing the acceptable use of information technology shall be documented.

- Acceptable Use Training: All employees shall undergo training, briefings, and orientation as deemed necessary by the circuit to support compliance with all elements of established acceptable use and applicable information security policies and guidelines.

- Remote Access Policy: Where applicable each circuit will maintain a written remote access policy.

- Sensitive and Exempt Data Handling: All employees with access to sensitive or exempt data shall be trained to handle the data in compliance with relevant guidelines. The Florida Department of Law Enforcement ("FDLE") establishes Criminal Justice Information System ("CJIS") guidelines governing the access by any workstations FCIC/NCIC data directly or through the Judicial Inquiry System ("JIS").

- Incident Response – Incident Response ("IR") procedures shall be developed and maintained. IR procedures will guide appropriate steps to take in response to breaches in devices, networks, or physical security.

Network Control

- Network: Network security encompasses preventing unauthorized access to the LAN and WAN that will be used to access judicial services.

- Device Resistance: All critical devices within the perimeter network shall be resistant to attack by 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. Network audit logs should be retained for a minimum of three months.

- 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. Remote access logs should be recorded for a minimum of three months. A centralized point of access is preferred.

- Wireless Network Security and Management: All wireless networks and devices shall be locally authorized by each circuit 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:

- An application to provide complete systems and network management throughout the enterprise environments, preferably including Active Directory ("AD") monitoring, Structured Query Language ("SQL") (or equivalent) database monitoring, and detailed and flexible reporting.
- Network management applications that are deployed and integrated to support network management requirements, including hub, switch and router management.
- SNMP compliant hardware; when in a Windows environment, Windows Management Instrumentation ("WMI") compliance is required.
- These tools that have the ability to monitor across VLANs, WANs, and disparate network architectures, including wireless networks.
- Either IPv4/IPv6 protocols.
- Tools should contain the ability to monitor, report, and block offending IP addresses or infected network segments.
- Network Quality of Service ("QoS") management utilities.
- Preference for SSH or SSL over telnet or html for network management tools.
- Traffic monitoring systems that 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 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 Windows Server Update Services ("WSUS")), and detailed, flexible reporting mechanisms.

Server Management tools should contain the following capabilities:

- SNMP-compliance.
- Ability to monitor server health, including disk, memory, process utilization, and when possible, power consumption.
- Lightweight Directory Access Protocol ("LDAP") support when 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.

When evaluating system management tools, administrators should consider the following criteria:

- For flexibility, site or enterprise licensing is preferred.
- "Agent-less" tools are not required, but may be preferred.
- Robust reporting/metrics functionality is preferred and strongly recommended.

- Email/text alerts for virus monitoring should be available for all systems.
- Remote management of network, desktops, and servers, provided software meets the established security standards, is preferred.

A health report should be periodically generated, and contain the following information when 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 baseline for video conferencing definition.

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.264 SIP multimedia standards.
- Audio conferencing must support G.711 audio compression.
- 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.

Any endpoint or Multi-Point Conference Unit (“MCU”) traversing the Internet should be considered “best effort”, given the circuit’s inability to manage all aspects of the connection, signal quality and clarity.

3.2.5 Court Reporting Technologies

Court Reporting Standards shall comply with CJIS Security Policy under the U.S. Department of Justice, Federal Bureau of Investigation when applicable.

Reference
Technical and Functional Standards for Digital Court Recording (last updated February 2015).

3.2.6 Technical Support

Skill sets needed to achieve technology objectives and provide support and maintenance should be defined.

On call is 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 or less as when the call for assistance was received, depending on the criticality of the environment (e.g., a case manager's printer error can be responded to the same day, but a network outage impacting first appearance or shelter hearings must be responded to more quickly).

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

- Network
- Security
- Audio Video
- ADA
- Communications
    - Data
    - Voice
- Training
- Web
    - Internet
    - Intranet
- Application Development

Other Considerations: Geographic distribution of serviced sites will impact service levels. Multi-county or large county circuits must factor travel time into 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

For criminal proceedings, 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. For Civil proceedings, equipment may be used if available; otherwise attorneys are responsible for providing equipment needed for evidence presentation.

Post a disclaimer on the circuit's website concerning the provided technology is recommended. An example is listed below:

> Courtroom technology is provided as a courtesy to the legal profession and court participants. While the court will make every effort to ensure the equipment is working properly, the court does not guarantee the reliability or availability of the equipment. It is presumed that anyone using courtroom technology is properly trained to do so. The court is not responsible to provide educational or technical support for these services. By using this technology, the user agrees to hold the court harmless for any equipment failure or corruption of data, for any court related proceeding, and to not seek to delay/reschedule of court proceedings due to same. Finally, users agree to be prepared to proceed without using technology should the circumstances warrant such action.

Infrastructure

When building new courtrooms, plans shall include conduit and cable paths to support existing and future technology. Raised flooring is recommended for courtrooms to allow for easy access. Floor boxes can be used to support future expansion. If using floor boxes, industry standard termination must be accommodated into the design of the floor boxes and the wiring practices. See Figure 7 for a typical courtroom design.

Courtroom Technology shall include the following

- Sound Reinforcement System / ADA Compliant hardware. Microphone locations should be discussed with Chief Judge to determine if hanging microphones, table top microphones, or if both types are needed in the courtrooms.
- ADA Assisted Listening Devices.
- Video display(s).
- 1 pan/tilt/zoom camera (minimum).
- Digital Court Recording (when applicable).
- LAN access for Judge and Clerk.

Recommended Optional Integrated Equipment

- Touch panel audio/visual control pad.
- Sidebar microphones (not amplified, but only available to DCR and/or Court Reporters.
- Video displays/Intelligent displays (capable of supporting different multi-media sources).
- Touch screen video displays (witness stand for evidence presentation).
- 4 pan/tilt/zoom cameras (suggested camera options: judge, witness, courtroom, and evidence/jury). The evidence camera should be mounted in the ceiling at a location that allows evidence to be placed underneath for presentation.
- Network access / Wi-Fi for participants.
- Remote interpreting A/V equipment.
- Video conferencing.
- Teleconferencing.
- VHS / DVD Player.
- Analog stereo audio, composite video, S-video, VGA, S/PDIF, component, and HDMI inputs and/or wireless media display devices (examples: Crestron Air Media, Apple TV), display port, and other industry standard connections.
- Media plate.
- Remote technical support and control.
- White noise cancellation for side bar conferences.
- Where needed, the microphones should be configured to work with the DCR.

Hearing Rooms/Chambers
While sounds systems may not be needed in all hearing room types, other equipment is essential. These rooms shall include the following:

- ADA assisted listening devices.
- Video display(s).
- 1 pan/tilt/zoom camera.
- DCR (pre-wired if possible).
- LAN access for judge and clerk.

Recommended Optional Hearing Room/Chamber Equipment

- Network access / Wi-Fi for participants.
- Remote interpreting A/V equipment.
- 1 pan/tilt/zoom camera.
- Video Conferencing.
- Teleconferencing.
- VHS / DVD player.
- Analog stereo audio, composite video, S-video, VGA, S/PDIF, component, and HDMI inputs and/or wireless media display devices (examples: Crestron Air Media,

Apple TV), display port, and other industry standard connections. These inputs can be installed in a floor box or wall plate.

- Remote technical support and control.

Optional Mobile Technology
If funding is unavailable for integrated courtroom technology solutions, mobile systems are recommended instead. Evidence presentation systems should be able to display a wide range of types/format/sizes of physical and digital evidence used in today's courtrooms. An evidence presentation system should include (but not be limited to) the following support components:

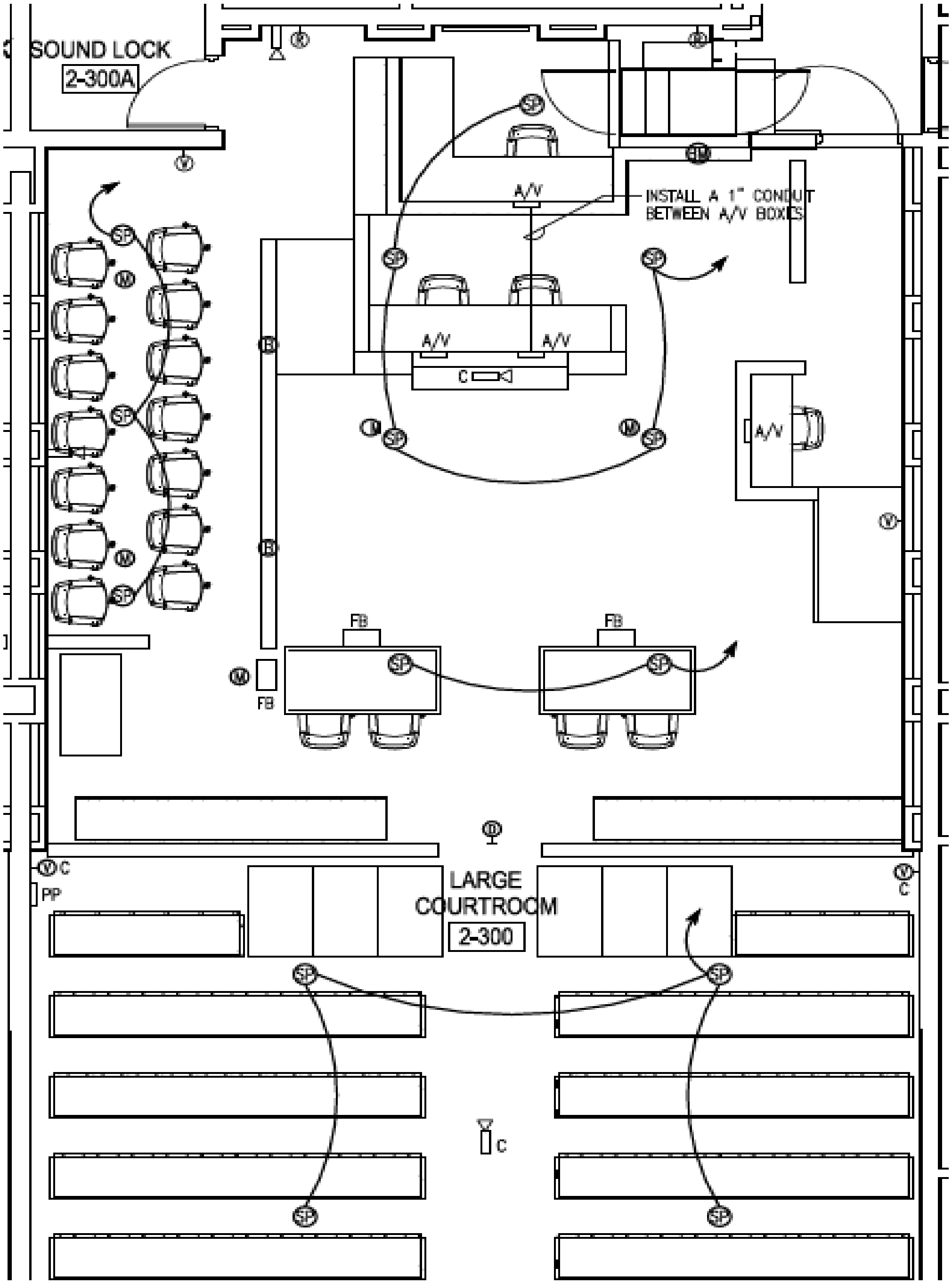
- **Display**
  Mobile display (TV/LCD screen) or projector:
  A mobile display is recommended only for smaller settings and should support multiple resolutions with sufficient lumens.

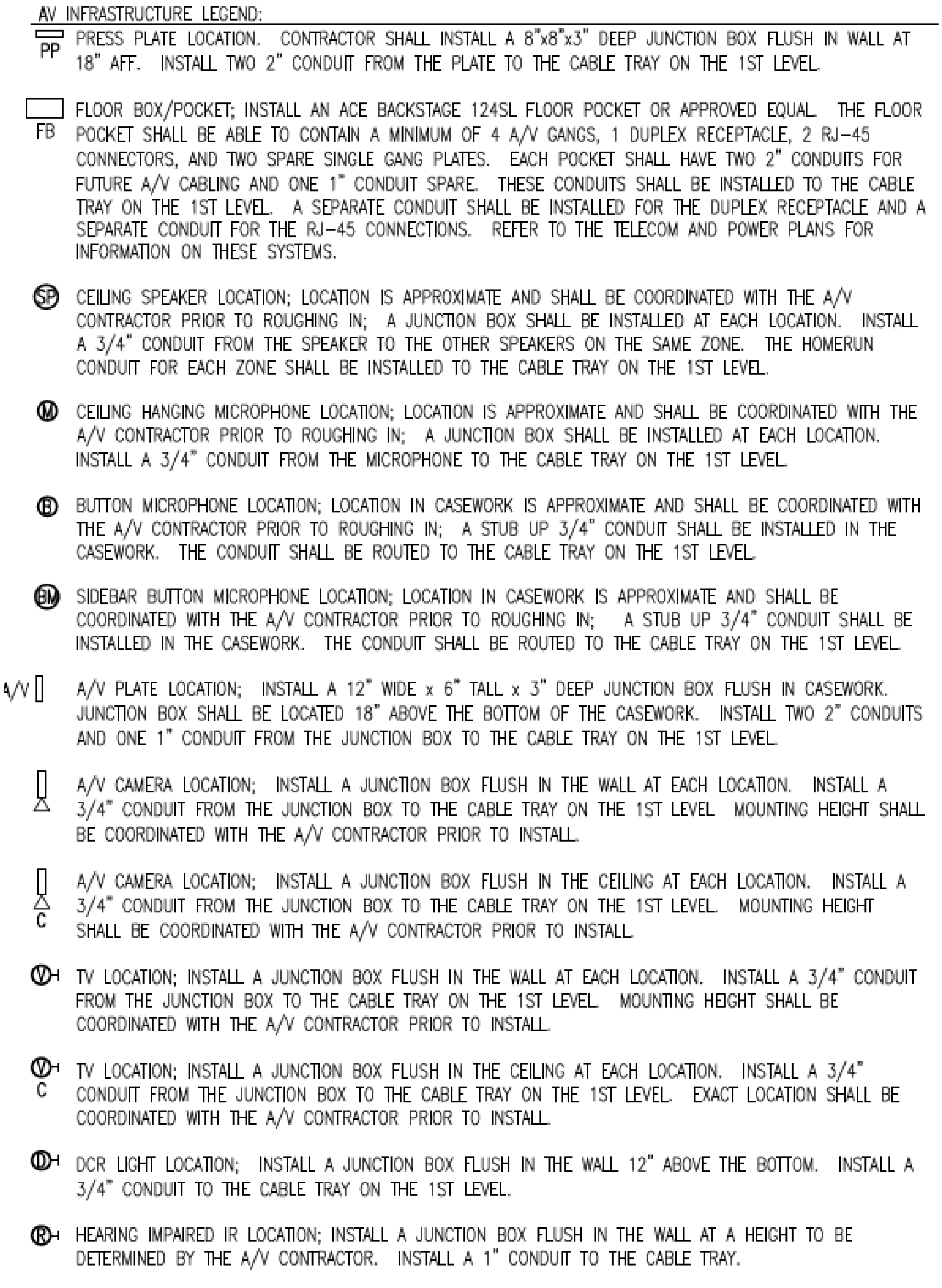
  A projector should support multiple resolutions with sufficient lumens for viewing in ambient light (will vary based upon projected image size) + projector screen.

  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, and 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, Blu-ray, and cell phone connectivity.
- **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, and OGG.
- **Overhead Projector**
- **Document Camera**

Figure 7. Courtroom Drawing





AV INFRASTRUCTURE LEGEND:

PP — PRESS PLATE LOCATION. CONTRACTOR SHALL INSTALL A 8"x8"x3" DEEP JUNCTION BOX FLUSH IN WALL AT 18" AFF. INSTALL TWO 2" CONDUIT FROM THE PLATE TO THE CABLE TRAY ON THE 1ST LEVEL.

FB — FLOOR BOX/POCKET; INSTALL AN ACE BACKSTAGE 124SL FLOOR POCKET OR APPROVED EQUAL. THE FLOOR POCKET SHALL BE ABLE TO CONTAIN A MINIMUM OF 4 A/V GANGS, 1 DUPLEX RECEPTACLE, 2 RJ-45 CONNECTORS, AND TWO SPARE SINGLE GANG PLATES. EACH POCKET SHALL HAVE TWO 2" CONDUITS FOR FUTURE A/V CABLING AND ONE 1" CONDUIT SPARE. THESE CONDUITS SHALL BE INSTALLED TO THE CABLE TRAY ON THE 1ST LEVEL. A SEPARATE CONDUIT SHALL BE INSTALLED FOR THE DUPLEX RECEPTACLE AND A SEPARATE CONDUIT FOR THE RJ-45 CONNECTIONS. REFER TO THE TELECOM AND POWER PLANS FOR INFORMATION ON THESE SYSTEMS.

SP — CEILING SPEAKER LOCATION; LOCATION IS APPROXIMATE AND SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO ROUGHING IN; A JUNCTION BOX SHALL BE INSTALLED AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE SPEAKER TO THE OTHER SPEAKERS ON THE SAME ZONE. THE HOMERUN CONDUIT FOR EACH ZONE SHALL BE INSTALLED TO THE CABLE TRAY ON THE 1ST LEVEL.

M — CEILING HANGING MICROPHONE LOCATION; LOCATION IS APPROXIMATE AND SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO ROUGHING IN; A JUNCTION BOX SHALL BE INSTALLED AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE MICROPHONE TO THE CABLE TRAY ON THE 1ST LEVEL.

B — BUTTON MICROPHONE LOCATION; LOCATION IN CASEWORK IS APPROXIMATE AND SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO ROUGHING IN; A STUB UP 3/4" CONDUIT SHALL BE INSTALLED IN THE CASEWORK. THE CONDUIT SHALL BE ROUTED TO THE CABLE TRAY ON THE 1ST LEVEL.

BM — SIDEBAR BUTTON MICROPHONE LOCATION; LOCATION IN CASEWORK IS APPROXIMATE AND SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO ROUGHING IN; A STUB UP 3/4" CONDUIT SHALL BE INSTALLED IN THE CASEWORK. THE CONDUIT SHALL BE ROUTED TO THE CABLE TRAY ON THE 1ST LEVEL.

A/V ▯ — A/V PLATE LOCATION; INSTALL A 12" WIDE x 6" TALL x 3" DEEP JUNCTION BOX FLUSH IN CASEWORK. JUNCTION BOX SHALL BE LOCATED 18" ABOVE THE BOTTOM OF THE CASEWORK. INSTALL TWO 2" CONDUITS AND ONE 1" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL.

A/V CAMERA LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE WALL AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL. MOUNTING HEIGHT SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO INSTALL.

C — A/V CAMERA LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE CEILING AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL. MOUNTING HEIGHT SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO INSTALL.

V — TV LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE WALL AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL. MOUNTING HEIGHT SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO INSTALL.

V C — TV LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE CEILING AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL. EXACT LOCATION SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO INSTALL.

D — DCR LIGHT LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE WALL 12" ABOVE THE BOTTOM. INSTALL A 3/4" CONDUIT TO THE CABLE TRAY ON THE 1ST LEVEL.

R — HEARING IMPAIRED IR LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE WALL AT A HEIGHT TO BE DETERMINED BY THE A/V CONTRACTOR. INSTALL A 1" CONDUIT TO THE CABLE TRAY.

3.3 Requirements for Interoperability and Data Exchange Standards

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 toward web based interfaces. Scanning systems and other applications that directly interface with peripherals are more difficult to move to web based applications, but it is possible.

The technical standards listed below have been developed across all industry sectors and have the joint backing of many software development companies (e.g., Microsoft, Oracle, Sybase, IBM) that have recognized that information exchange and the resulting gains in productivity and efficiency are critical strategic goals of improved system performance.

- Software applications must support the following standards when applicable:
  - 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 should access 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.
    - JSON ("Java Script Object Notation").
    - 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 should 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 should use industry-proven algorithms, techniques, platform-supplied infrastructure, and vendor-tested and supported technologies.

3.3.1 Data Transmission

Protocols for transmission, between distinct entities, of data governed by this document must be generally available, nonproprietary, and protected by the most secure methods reasonably available to all participants. Each repository of data shall provide its data in accordance with this document, the Data Exchange Standards, and such other standards as may be adopted under the authority of the Supreme Court.

3.3.2 Database Standards

Database connectivity to some databases may not be possible due to driver/network restrictions at the location. Each participating agency/entity should collaboratively develop a plan governing the connection to, accessing, and formatting the data maintained in the particular database source. These databases should:

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

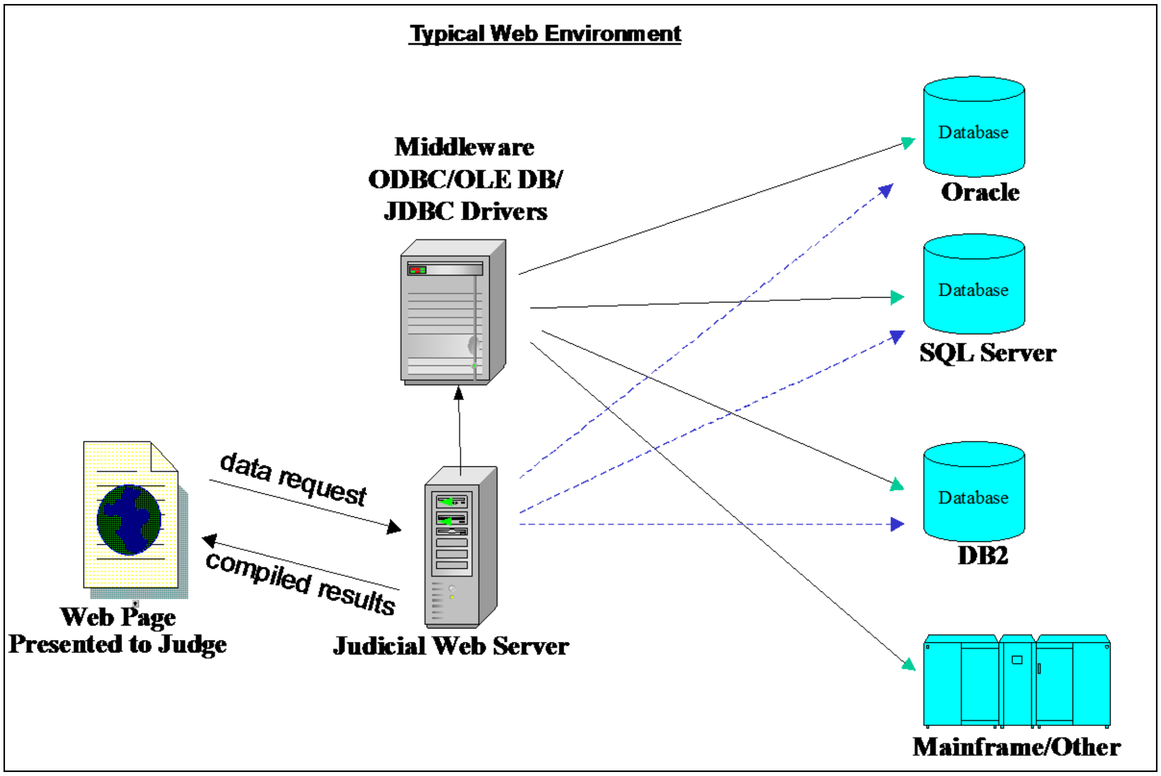
3.3.3 Database Connectivity

A detailed system architecture should be defined that will meet the business requirements of judicial applications. 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”)
- Java Database Connectivity (“JDBC”).
- Database Native Drivers

Figure 8. Conceptual Data Exchange Environment



3.3.4 Archival Storage of Electronic Documents

Electronic document image systems must accommodate the need to archive electronic images in a manner that will guarantee high fidelity rendering of that image in the present system as well as future systems and their storage format changes. Archival storage requirements of electronic media may range for 1 to 10 years, and each system must consider and address the challenges of delivering images seamlessly, without loss of fidelity, as changes occur over time. Archival storage formats used must be able to meet long term rendering requirements as well has have a method to meet ADA requirements/accommodations. An industry standard specifically developed for long term archival purposes is PDF/A. Where possible PDF/A is strongly encouraged. Other archival formats may also be used as long as they meet the fidelity and ADA requirements.

To address these issues, the PDF/A document format was created by the Association for Suppliers of Printing, Publishing and Converting Technologies and the Association for Information and

Image Management, and ratified by the International Standards Organization as standard ISO 19005. PDF/A is a restricted version of the popular PDF file format that helps ensure long-term retrieval.

Numerous agencies and institutions, including the U.S. Federal Court, are adopting PDF/A as their primary method of electronic document storage. A current listing is available at http://www.pdfa.org/2011/06/recommendations-for-pdfa/

3.3.5 Access to Court Data and Documents

The clerk shall provide access to local data and local document images to the court. Access to data and document images can be accomplished directly via the local document image store, a real time replica of same, or a local web service. The chief judge of the circuit and the clerk of court of the respective county shall determine the development and maintenance specifications necessary to provide the requested data and document images. Costs associated with hardware, software, or creating the replicated database and maintenance specifications and the responsibility for payment of such costs shall be determined upon mutual agreement by the chief judge and the clerk.

3.4 Cloud Computing

There are unique opportunities and challenges with the advent of Cloud Computing. Cloud services are evolving at a fast pace that go beyond file storage.

3.4.1 Approval Process

Due to the changing nature of cloud computing in the areas of storage and service offerings, moving the cloud can be beneficial financially, but also carries many risks. Therefore, the Chief Judge shall be informed of benefits and potential risks, and give approval before court records or court services are moved to a cloud service provider. Where applicable, cloud services must conform to CJIS standards.

Before court records/services are moved to a cloud service provider, the court or clerk of court shall provide a letter and migration plan to the Florida Courts Technology Commission (“FCTC”) detailing the intended move, along with signature confirmation that the chief judge has reviewed and approved the migration.

3.4.2 Risks

- One of the major risks with cloud computing involves the accessibility of data/services upon termination of the hosting agreement due to formatting or proprietary storage protocols implemented by the vendor. Care should be given to ensure the data is returned in the same format in which it was migrated. Security and integrity of the court data may be at risk when a contracted cloud service provider, who is also responsible for data security, is storing the data outside the monitoring capability of court/clerk staff. Care must be taken to ensure the security and integrity of court data and services. Security audits and reviews should be conducted. Security breaches should be properly and immediately reported. In all instances, the data will remain the property of the applicable jurisdiction within the State of Florida.

- Because SLAs can change often and with short notice, it is important that a plan be in place to monitor and audit the impact that such changes to agreements could have, and mitigate their impact.

3.4.3 Storage Restrictions

The location of cloud data storage is restricted based on the classifications below.

- Classification 1: Judicial Branch Records as defined in Florida Rules of Judicial Administration 2.420(b)(1):
  - Court Records
  - Administrative Records
- Classification 2: Logs (e.g., temporary files such as computer activity logs, scheduling polls that are short term files).

Data in classification 1 must reside within the United States, with the master copy as that term is defined by Florida law residing within the State of Florida. This will ensure jurisdiction remains within Florida. Data in classification 1 shall be encrypted, both in transit and at rest.

Data in classification 2 may be stored outside the United States, but the data must be stored in such a way as to facilitate copying of the data or a portion thereof in an amount of time similar to the amount of time such duplication would take if the data were stored within the State of Florida. The data must be available for such duplication for a time period at least as long as the applicable records retention period provided by Florida law.

3.4.4 Best Practices

Best practices related to the security and integrity of data stored in the cloud should be followed either by practice (as identified in proposed cloud migration plans) or by contractual agreement. These include, but are not limited to:

- Encryption may be required for some types of email at rest and in route.
- Data encryption should be considered for storage of sensitive data on the cloud.
- Any agreement should include a clause prohibiting the use of court data for advertising or marketing, or any other use without the express written consent of the governing jurisdiction.
- Any agreement should include a clause requiring law enforcement to work through the custodian of the record when requesting access to records rather than direct access.

3.4.5 Resources

- ISO 27018:2014 Compliant Cloud data privacy

- Security
    - Cloud Security Alliance: Cloud Control Matrix
    - PCI Security Standards
    - ISO/IEC 27001:2013
    - ISO/IEC 27002:2013
- Justice Partner Compliance
    - Criminal Justice Information Services (CJIS) compliance
    - Compliance with Justice Partner standards for current & future integrations
- Industry-verified conformity with global standards