ADMINISTRATIVE **O**FFICE OF THE **C**OURTS	**ISC VENDOR SECURITY REQUIREMENTS**	State of IDAHO JUDICIAL BRANCH

		Compliant?				
#	ISC Security Requirements	Yes	No	N/A	Description in Detail	Reference
1	Are modern cryptographic modules consistently used where cryptography is required?					**Associated NIST Controls** Remote Access | Protection of Confidentiality and Integrity Using Encryption [AC-17 (2)] Access Restrictions for Change | Signed Components [CM-5 (3)] Authenticator Management | Password-Based Authentication [IA-5 (1)] Transmission Confidentiality and Integrity | Cryptographic Protection [SC-8 (1)] Cryptographic Key Establishment and Management [SC-12] Cryptographic Key Establishment and Management | Symmetric Keys [SC-12 (2)] Cryptographic Key Establishment and Management | Asymmetric Keys [SC-12 (3)] Protection of Information at Rest [SC-28] **Minimum Required Encryption Cipher Strength** AES-256 AES-128 **Required Encryption-In-Transit Protocols** TLS 1.1 (Compliant) TLS 1.2 (Compliant)

2	Can the system support Single Sign On (SSO)?					**Associated NIST Control** Identification and Authentication (Non-Organizational Users) [IA-8]
3	Does the Service Provider (SP) scan for and consistently remediate High vulnerabilities within 30 days, Moderate vulnerabilities within 90 days, and Low vulnerabilities within 180 days? Please note framework used to determine vulnerability criticality.					**Associated NIST Control** Vulnerability Scanning [RA-5] **Required** Credentialed scans must be used on all devices, and the credentials used must be validated to work properly for scanning purposes.
4	Does the SP and system utilize an audit and event monitoring solution that can support 90 days of online storage and 365 days of event/log data?					**Associated NIST Controls** Event Logging [AU-2]Content of Audit Records [AU-3]Time Stamps [AU-8]Audit Record Retention [AU-11] **Required** Some form of log aggregation is required. A SIEM is recommended but not required.

5	Does the system's external DNS solution support DNS Security (DNSSEC) to provide origin authentication and integrity verification assurances?					**Associated NIST Controls** Secure Name/Address Resolution Service (Auth. Source) [SC-20] Secure Name/Address Resolution Service (Recursive or Caching Resolver) [SC-21]
6	Does the system require multi-factor authentication (MFA) for administrative accounts and functions?					**Associated NIST Controls** Identification and Authentication (Organizational Users) [IA-2] Identification and Authentication | MFA for Privileged Accounts [IA-2(1)] Identification and Authentication | Local Access to Privileged Accounts [IA-2(3)]
7	Does the system ensure secure separation of customer data?					**Associated NIST Control** Information Flow Enforcement [SC-4]

8	Does the system have the capability to detect, contain, and eradicate malicious software?					**Associated NIST Controls** Maintenance Tools | Inspect Media [MA-3 (2)] Malicious Code Protection [SI-3] Malicious Code Protection | Central Management [SI-3 (1)] Malicious Code Protection | Automatic Updates [SI-3 (2)] Malicious Code Protection | Non-signature Based Detection [SI-3 (7)]
9	Does the system protect audit information from unauthorized access, modification, and deletion?					**Associated NIST Controls** Audit Reduction and Report Generation [AU-7]Protection of Audit Information [AU-9]
10	Does the SP have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? Detail recovery times for outages.					**Associated NIST Controls** Contingency Plan [CP-2] Contingency Plan | Capacity Planning [CP-2 (2)] Contingency Plan | Resume Mission and Business Functions [CP-2 (3)] System Backup [CP-9] System Recovery and Reconstitution [CP-10]

11	Does the SP maintain a current, complete, and accurate inventory of the information system software, hardware, and network components?					**Associated NIST Control** System Component Inventory [CM-8]
12	Does the SP follow a formal change control process that includes a security impact assessment?					**Associated NIST Controls** Configuration Change Control [CM-3] Impact Analysis [CM-4]
13	Does the SP employ automated mechanisms to detect inventory and configuration changes?					**Associated NIST Controls** Baseline Configuration | Automation [CM-2(2)] Configuration Settings | Automated Mgmt., Application & Verification [CM-6(1)] System Component Inventory | Automated Unauthorized Component Detection [CM-8(3)]
14	Does the SP prevent unauthorized changes to the system?					**Associated NIST Controls** Access Restriction for Change [CM-5] Access Restriction for Change | Automated Access Enforcement & Audit Records [CM-5(1)] Access Restriction for Change | Privilege Limitation for Production and Operation [CM-5(5)]

15	Does the SP scan for configuration settings on systems in the environment?					**Associated NIST Controls** Configuration Settings [CM-6] **Preference** SCAP scans
16	Does the SP have an Incident Response Plan?					**Associated NIST Control** Incident Response Testing [IR-3]
17	Does the SP have a Configuration Management Plan?					**Associated NIST Controls** Configuration Management Plan [CM-9] User-Installed Software [CM-11]
18	Does the SP have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34?					**Associated NIST Controls** Contingency Plan [CP-2] Telecommunications Services [CP-8]
19	Does the SP conduct code analysis for internally developed code?					**Associated NIST Control** Developer Testing and Evaluation [SA-11]

For the following, please note is the system leverages a StateRAMP or FedRAMP accredited IaaS.
Please provide letter of certification from the leveraged system's service provider.

20	Does the SP restrict physical system access to only authorized personnel?					**Associated NIST Controls** Physical Access Authorizations [PE-2] Physical Access Control [PE-3] Access Control for Transmission [PE-4] Access Control for Output Devices [PE-5] Monitoring Physical Access [PE-6] Visitor Access Records [PE-8]
21	Does the SP monitor and log physical access to the information system and maintain access records?					**Associated NIST Controls** Monitoring Physical Access [PE-6]Visitor Access Records [PE-8]

22	Does the SP monitor and respond to physical intrusion alarms and surveillance equipment?					**Associated NIST Control** Monitoring Physical Access | Intrusion Alarms & Surveillance Equipment [PE-6 (1)]
23	Does the system have or use alternate telecommunications providers?					**Associated NIST Controls** Telecommunication Services [CP-8] Telecommunication Services | Single Point of Failure [CP-8 (2)]
24	Does the system have backup power generation or other redundancy?					**Associated NIST Controls** Emergency Power [PE-11]

25	Does the SP have service level agreements (SLAs) in place with all telecommunications providers?					**Associated NIST Control**Telecommunications Services | Priority of Service Provisions [CP-8 (1)]

PROVIDE THE ADDITIONAL DOCUMENTS.

		Attached			
#	ISC Minimum Documentation	Yes	No	N/A	Notes
1	Solution Diagram				
2	Data Flow Diagram				
3	Roles & Permissions				
4	System Security Plan				
5	Continuous Monitoring Plan				
6	User Guide				
7	Policies and Procedures (link or attachment)				