| 1. BASIC INFORMATION | |
|---|---|
| **SAPA Transmission Sensitive Information**. Information provided to supplier by SAPA Transmission or created by the supplier on behalf of SAPA Transmission during the course of business including: SAPA Transmission' Proprietary Information, 3rd Party / Customer Proprietary Information, Personal / Personally Identifiable Information, CUI and Export Controlled Information. | |
| Company Name | |
| Address | |
| IT Contact Person | |
| Email | |
| Phone | |
| Date of completion | |

| 2. SUPPLIERS CYBERSECURITY QUESTIONNAIRE | Yes | No | Comments |
|---|---|---|---|
| 2.1 Does your company have cybersecurity policies based on industry standards (ISO 27001, NIST 800-53) and require they be used to manage IT devices that process or store sensitive information? | ○ | ○ | |
| 2.2 Does your company protect sensitive information during transmission between the owning third-party as well as other parties with whom that data is shared (i.e., Encryption, SSL/TLS connections)? | ○ | ○ | |
| 2.3 Are devices that store or process sensitive information protected from the Internet by a firewall? | ○ | ○ | |
| 2.4 Does your company have a dedicated, full-time employee or subcontracted IT staff? | ○ | ○ | |
| 2.5 Does your company have a dedicated employee or subcontracted cybersecurity staff? | ○ | ○ | |
| 2.6 Does your company have a cybersecurity user education and awareness program? | ○ | ○ | |
| 2.7 Does your company perform cybersecurity audits by objective internal employees or external 3rd parties on IT systems/devices and IT services that store or process sensitive information at least annually? | ○ | ○ | |
| 2.8 Do all devices that store or process sensitive information at a minimum have commercially available antivirus with current signature files? | ○ | ○ | |
| 2.9 Do all devices that store or process sensitive information at a minimum have a unique username and complex password to access the system? | ○ | ○ | |
| 2.10 Do the devices that store or process sensitive information at a minimum have access control that is configured on a least privilege model (a person only has access to the data/device that they need)? | ○ | ○ | |
| 2.11 Do all devices that store or process sensitive information at a minimum have vulnerability scanning performed at least monthly AND are vulnerabilities being remediated in a risk-based priority (highest priority vulnerabilities are fixed first)? | ○ | ○ | |
| 2.12 Do all devices that store or process sensitive information at a minimum have all unnecessary ports and services disabled and the device is used for limited functions (ex. A device acting solely as a file server vs. a file server, FTP server, and web server)? | ○ | ○ | |

| 2. SUPPLIERS CYBERSECURITY QUESTIONNAIRE | Yes | No | Comments |
|---|---|---|---|
| 2.13 Do all devices that store or process sensitive information at a minimum have patches deployed for high-risk operating system and third-party application vulnerabilities within industry best practices (i.e., 48 hours) and medium/low risk patches to be deployed in less than 30 days? | ○ | ○ | |
| 2.14 Are all laptop devices that store sensitive information encrypted? | ○ | ○ | |
| 2.15 Do all mobile devices (smartphones, tablets) that store sensitive information at a minimum have configuration management provided by a company owned centrally managed infrastructure?<br>Note: For IT environments with no mobile devices, answer Yes | ○ | ○ | |
| 2.16 Do all mobile devices (smartphones, tablets) that store sensitive information at a minimum have access control to the device (complex password to access device)?<br>Note: For IT environments with no mobile devices, answer Yes | ○ | ○ | |
| 2.17 Do all mobile devices (smartphones, tablets) that store sensitive information at a minimum have the ability to remotely wipe the device?<br>Note: For IT environments with no mobile devices, answer Yes | ○ | ○ | |
| 2.18 Does your company have a Computer Incident Response Team with a formal process to respond to cyber-attacks? | ○ | ○ | |
| 2.19 When your company must share sensitive information, does your company require the suppliers to follow policies for cybersecurity based on industry standards (e.g., ISO 27001, NIST 800-53)? | ○ | ○ | |
| 2.20 Does your company require a 2-factor authentication for remote access (e.g., token used in addition to a username and password for VPN login)?<br>Note: For IT environments with no remote access, answer Yes | ○ | ○ | |
| 2.21 Does your company perform industry standard (e.g., ISO 27001, NIST 800-53) logging and monitoring on devices that store or process sensitive information? | ○ | ○ | |
| 2.22 Does your company control web access based on the risk (e.g., reputation, content, and security) of the sites being visited (e.g., Web Proxy Controls)? | ○ | ○ | |
| 2.23 Does your company have capabilities of detecting and blocking malicious e-mail prior to delivery to the end-user? | ○ | ○ | |
| 2.24 Does your company have tools and processes to mitigate Advanced Persistent Threat (APT) attacks? | ○ | ○ | |
| 2.25 Does your company perform full packet capture? | ○ | ○ | |
| 2.26 Does your company actively participate in a cyber intelligence sharing forum? (e.g., CISP, ADMIE, MSPIE or other CPNI Information Exchange) | ○ | ○ | |
| 2.27 Does your company have a team (employee or subcontracted) that is capable of performing forensics in support of investigations? | ○ | ○ | |