Attachment A

to

RFP No. 5026

for the

STATE OF MISSISSIPPI

Cybersecurity EPO

ITS Project No. 49741

Technical Specifications

1. Cybersecurity Product and Service Categories

Listed below is a summary of the categories of products and services that may be solicited under this EPO.

1.1. Endpoint & Device Security

1.1.1. Includes products, services, and support for protecting endpoints and devices from threats. Examples include but are not limited to:

1.1.1.1. Endpoint Detection and Response (EDR)

1.1.1.2. Antivirus and anti-malware solutions

1.1.1.3. Endpoint management and security

1.1.1.4. Endpoint encryption

1.1.1.5. Mobile device security

1.1.1.6. Endpoint vulnerability management

1.1.1.7. Endpoint security implementation and support

1.1.2. For solutions that will be deployed within the Enterprise State Network (ESN), those solutions must function within the ESN and adhere to standards and policies defined by ITS.

1.2. Network & Perimeter Security

1.2.1. Includes products, services, and support designed to protect network infrastructure and network boundaries from unauthorized access or other cybersecurity threats. Examples include but are not limited to:

1.2.1.1. Firewalls

1.2.1.2. Intrusion Detection and Prevention Systems (IDS/IPS)

1.2.1.3. Network Access Control (NAC)

1.2.1.4. Virtual Private Network (VPN) security

1.2.1.4.1. Excluding agencies who are on the state network and are required to participate in the Enterprise VPN solution

1.2.1.5. Network segmentation

1.2.1.6. DDoS protection

1.2.1.6.1. Excluding HTTP and HTTPS traffic as it has inherent DDoS protection through the Enterprise Cloud Security Border

1.2.2. For solutions that will be deployed within the Enterprise State Network (ESN), those solutions must function within the ESN and adhere to standards and policies defined by ITS.

1.3. Cloud & Application Security

1.3.1. Includes products, services, and support designed to protect cloud environments, applications, and cloud infrastructure. Examples include but are not limited to:

1.3.1.1. Cloud Security Posture Management

1.3.1.2. Cloud workload security

1.3.1.3. Container and cloud security

1.3.1.4. Web Application Firewalls (WAF)

1.3.1.4.1. Excluding agencies who are on the state network and are required to participate in the Enterprise Cloud Security Border

1.3.1.5. API security

1.3.1.5.1. Excluding agencies who are on the state network and are required to participate in the Enterprise Cloud Security Border

1.3.2. For solutions that will be deployed within the Enterprise State Network (ESN), those solutions must function within the ESN and adhere to standards and policies defined by ITS.

1.4. Messaging & Collaboration Security

1.4.1. Includes products, services, and support designed to protect email, messaging systems, collaboration platforms, and associated communications. Examples include but are not limited to:

1.4.1.1. Email security gateways

1.4.1.2. Spam and malware filtering

1.4.1.3. Phishing and Business Email Compromise (BED) protection

1.4.1.4. Email authentication and security

1.4.1.5. Collaboration platform security

1.4.1.6. Malicious link and attachment protection

1.4.2. Excludes agencies who are on the state network and are required to participate in the Enterprise Email Gateway

1.5. Monitoring & Threat Detection

1.5.1. Includes products, services, and support designed to identify, analyze, investigate, and respond to cybersecurity threats and events. Examples include but are not limited to:

1.5.1.1. Security Information and Event Management (SIEM)

1.5.1.2. Security Operations Center (SOC) services

1.5.1.3. Managed Detection and Response (MDR)

1.5.1.4. Threat intelligence and threat hunting

1.5.1.5. Extended Detection and Response (XDR)

1.5.1.6. Security monitoring and support

1.5.2. For solutions that will be deployed within the Enterprise State Network (ESN), those solutions must function within the ESN and adhere to standards and policies defined by ITS.

1.6. Data Protection & Resilience

1.6.1. Includes products, services, and support designed to protect data from unauthorized access, modification, loss, or disruption and to support the recovery and continued availability of information systems. Examples include but are not limited to:

1.6.1.1. Data Loss Prevention (DLP)

1.6.1.2. Data encryption and key management

1.6.1.3. Data classification and discovery

1.6.1.4. Backup and recovery

1.6.1.5. Business resilience plan and recovery

1.6.1.6. Ransomware protection and recovery

1.6.2. For solutions that will be deployed within the Enterprise State Network (ESN), those solutions must function within the ESN and adhere to standards and policies defined by ITS.

1.7. Incident Response Services

1.7.1. Incident Response services provide proactive readiness capabilities through retainer-based engagements and reactive support in response to cybersecurity incidents, augmenting your agency's internal capacity to prepare for, detect, contain, and recover from security events.

1.7.1.1. Provides proactive retainer-based services. These services provide proactive readiness activities (maturity assessments, tabletop exercises, playbook development)

1.7.1.2. Provides reactive services and support to triage and establish the incident to determine scope of the incident. Reactive incident support including investigation, containment, forensic analysis, recovery coordination, breach coach integration, and ransomware protection and recovery

1.7.2. For solutions that will be deployed within the Enterprise State Network (ESN), those solutions must function within the ESN and adhere to standards and policies defined by ITS.

1.8. Security Assessment Services

1.8.1. Includes services focused on evaluation cybersecurity controls and identifying vulnerabilities.

1.8.2. Types of testing included:

1.8.2.1. Cloud Compliance Testing

1.8.2.2. Penetration Testing

1.8.2.3. Security Risk Assessment

Note: ITS intends to combine this category with vendors from another RFP (RFP 4350). Customers will solicit all vendors within the combined category EXCEPT for projects that are specifically for agencies who need to comply with the Enterprise Security Policy. As of the release of this RFP, only 4350 vendors are approved to supply agencies with ESP compliance reports. All other projects will be available for all vendors.

If you are interested in being approved to provide ESP compliance reports, contact ITS for information on how you can be certified.

2. Global Requirements

2.1. Items outside of ITS purview are not part of this EPO

2.2. Freight must be Freight on Board (FOB) Destination for a standard delivery. If the delivery is beyond a standard delivery such as “white glove treatment” or because of weight/size, the freight/transportation charges may be line-items

2.3. Individual parts or components are allowed and are part of the category of the equipment they are being purchased to upgrade or repair

2.4. Installation services, training, extended and separate warranties, maintenance agreements, and repair services are allowed if they are for products or services within a category covered by this RFP. These are considered part of the relevant category or categories. These services should not cover any solutions that are not within the scope of this EPO.

2.5. Solutions designated for use outside the United States are excluded

2.6. Solutions including cellular service plans are excluded

2.7. Solutions designed for home use are excluded

2.8. Products must be new

3. Warranty

3.1. General Warranty Requirements and Definitions

3.1.1. Vendor most provide a minimum one-year warranty covering all parts and labor to correct any defect in the proposed equipment. This warranty period must become effective from the delivery date of Vendor's products/services

3.1.2. If an "On-Site warranty is proposed, the warrantor will, without charge, repair or replace a defective product. During the "on-site" period, the warrantor must come to the customer's site to repair or pick-up the defective product

3.1.3. If a "Parts and Labor" warranty is proposed, the warrantor must replace or repair the defective product, but it is the customer's responsibility to return the defective product to the warrantor for repair. This includes "return to depot", "carry-in", or "shipping to warrantor", subject to shipping charges as defined below

3.1.4. The warranty must include the BASE Product and any items purchased with the base product

3.1.5. The "BASE Product" includes the components required to meet the minimum specifications as outlined for each of the categories

3.1.6. The "Internal EPL Components" are those selected from the EPO options at the time of purchase that are internal to the product

3.1.7. Non-EPO items are not automatically covered in the BASE Product or as an EPO Component purchased with the base product. Customer and Seller must negotiate a warranty separately if needed. NOTE: Vendor-defined options in any open-ended specifications are EPO items

3.1.8. Charges for shipping and handling must be borne by the Seller during the on-site warranty period or for the first year of the warranty if the items are not covered by an on-site warranty

3.1.9. After the expiration of the first year (for items without on-site coverage) or of the on-site warranty period and for the remainder of the warranty period, Seller is required to pay shipping from the manufacturer or repair facility back to the customer, however, Seller is not required to pay shipping from the customer to the manufacturer or repair facility

3.2. Seller will warrant software against defects in workmanship of product for a period of ninety (90) days from the date of sale of the licensed software or the system on which the software is loaded, whichever is applicable