ADVERTISEMENT
FOR THE USE AND BENEFIT OF
NESHOBA COUNTY, MISSISSIPPI

The NESHOBA COUNTY BOARD OF SUPERVISORS will receive sealed proposals until Wednesday, October 28, 2026 at 12:00 PM from qualified vendors in response to this solicitation for acquiring the following services:

Managed Cybersecurity Services

Detailed specifications for the above-described services and bid forms may be obtained from the Neshoba County Board of Supervisors office at the Neshoba County Courthouse, 401 Beacon Street, Suite 201, Philadelphia, Mississippi 39350, by calling 601-656-6281 or on Neshoba County's website at www.neshobacounty.net. Neshoba County, Mississippi will determine if compliance with the specifications exist before accepting any bid.

INSTRUCTIONS TO BIDDERS:

The detailed proposal, with the pricing proposal, in response to this solicitation shall be submitted via single file PDF under the correct bid solicitation at www.neshobacounty.net/bids or be placed in a sealed envelope marked "2026 Managed Cybersecurity Services" and filed with the Neshoba County Board of Supervisors C/O Chancery Clerk Gidget Stovall Tate, 401 Beacon Street, Suite 107, Philadelphia, Mississippi 39350 by 12:00 PM on Wednesday, October 28, 2026. Neshoba County will not be responsible for opening of proposals not properly marked or received after the proposal response date and time.

It shall be incumbent upon each bidder to understand the specifications as listed herein and to obtain clarification when necessary. It is not the intent of these specifications to limit the bidding to any particular provider of services, but rather to select such services to provide for specific needs and specific tasks.

Published by Order of the Board of Supervisors of Neshoba County, Mississippi on the 21st day of September 2026.

/s/_GIDGET STOVALL TATE
GIDGET STOVALL TATE, CLERK
BOARD OF SUPERVISORS
NESHOBA COUNTY, MISSISSIPPI

NESHOBA COUNTY BOARD OF SUPERVISORS

REQUEST FOR PROPOSALS

MANAGED CYBERSECURITY SERVICES

Issue Date: September 21, 2026

Proposal Due Date/Time: Wednesday, October 28, 2026 at 12:00 PM

Contract Period: Twelve (12) Months

Neshoba County Board of Supervisors

401 E. Beacon Street, Suite 201

Philadelphia, Mississippi 39350

Telephone: (601) 656-6281

Email: info@neshobacounty.net

NOTICE OF REQUEST FOR PROPOSALS

Neshoba County, Mississippi, through its Board of Supervisors, is soliciting competitive sealed proposals from qualified cybersecurity service providers to furnish twelve (12) months of Managed Cybersecurity Services to enhance the cyber security posture and preparedness of the County.

The County intends to procure a contracted managed-service provider capable of delivering vCISO, Security Operations Center (SOC), and Cyber Security Engineering services to establish, maintain, monitor, measure, and improve a comprehensive cybersecurity program. The services shall specifically support the County in addressing the cybersecurity goals identified in the CISA Cross-Sector Cybersecurity Performance Goals (CPGs) and specifically the CPG 2.0.

Proposals shall be prepared and submitted in accordance with the Request for Proposals (RFP). Proposers shall provide a firm twelve-month price and a clear description of all services included. Payment shall be made for services on a monthly basis.

The County reserves the right to reject any or all proposals, to waive informalities or irregularities, to request clarification, to conduct interviews or demonstrations, and to award a contract in the best interest of the County.

PROPOSAL SUBMISSION

Item	Requirement
Submission Method	Sealed proposal delivered to the County at Neshoba County Board of Supervisors, C/O Chancery Clerk Gidget Tate, 401 E Beacon Street, Suite 107, Philadelphia, MS 39350 or via electronic submission at www.neshobacounty.net/bids under the correct solicitation response.
Number of Copies	One (1) original paper copy and one (1) searchable PDF on standard USB drive if delivered via sealed paper submission. If submitted electronically, one (1) original submission via single file PDF format.
Sealed Bid Envelope Marking	RFP – Managed Cybersecurity Services
Deadline	Wednesday, October 28, 2026 at 12:00 PM Central Time
Questions	Written questions must be submitted by 12:00 PM on Wednesday, October 21, 2026.
County Contact	County Administrator, 401 E. Beacon Street, Suite 201, Philadelphia, MS 39350 or via email to info@neshobacounty.net.

1. INTRODUCTION AND BACKGROUND

Neshoba County is a Mississippi County government seeking to strengthen its cybersecurity posture through professional managed cybersecurity services. The project is intended to procure and support a qualified third-party managed-service provider for a twelve-month period.

Cyber Security grant funds have been awarded to Neshoba County in support of this project from the Mississippi Office of Homeland Security and the grant project description includes professional services including the following: vCISO, SOC, and Security Engineering services. The project includes, among other services, a CPG Assessment; development/update of the County's Information Security Policy; development/update of the Disaster Recovery/Incident Response Plan; a cybersecurity tabletop exercise; daily, weekly, monthly, and/or quarterly optimization checks; and comprehensive attention to the CISA CPG goals.

The County is seeking a provider that can function as an extension of the County's technology and administrative resources and provide both strategic cybersecurity leadership, planning and practical technical support. The selected provider shall work cooperatively with the County, contracted IT providers, department heads, and other authorized personnel in formulating a comprehensive cyber security program and readiness posture.

2. PROJECT OBJECTIVES

- Establish a measurable, risk-informed cybersecurity program for the County.
- Provide cybersecurity monitoring, security engineering, maintenance, advisory, and support services.
- Provide vCISO-level governance and strategic cybersecurity leadership.
- Provide SOC capabilities sufficient to monitor, triage, investigate, escalate, and document security events.
- Assess the County's cybersecurity posture against the applicable CISA CPGs and establish a documented improvement roadmap.
- Maintain and improve the County's information security policies, incident response/disaster recovery documentation, and supporting procedures.
- Conduct a cybersecurity tabletop exercise and document lessons learned and corrective actions.
- Perform recurring monitoring, security and optimization activities.
- Track progress against CISA CPG goals and document evidence of implementation or a documented risk-based exception.
- Produce management-level reporting that allows the County to demonstrate grant-related progress and make informed cybersecurity decisions.

3. SCOPE OF SERVICES

The selected Contractor shall provide, at a minimum, the following services. Proposals may offer additional services at no additional cost when they materially improve the County's cybersecurity posture, but all required services must be included in the base twelve-month price.

3.1 Virtual Chief Information Security Officer (vCISO)

- Provide an assigned vCISO or equivalent senior cybersecurity executive as the County's primary strategic cybersecurity advisor.
- Conduct an initial cybersecurity program review and establish a twelve-month cybersecurity improvement roadmap.
- Conduct recurring management reviews with the County at least monthly, with additional meetings as reasonably required for incidents or significant security matters.
- Advise County leadership concerning cybersecurity risks, priorities, policies, technology, compliance, incident readiness, and resource requirements.
- Maintain a risk register identifying material cybersecurity risks, recommended mitigations, responsible parties, status, and target dates.
- Provide an executive-level monthly report summarizing cybersecurity posture, material risks, incidents, unresolved findings, CPG progress, and recommended actions.

3.2 Security Operations Center (SOC) / Managed Monitoring

- Provide managed security monitoring and SOC services appropriate for the County's environment.
- Monitor available security telemetry, including endpoint, network, identity, cloud, firewall, email, authentication, and other security sources made available by the County.
- Perform alert triage, investigation, escalation, and documentation.
- Provide defined severity levels and response/escalation procedures.
- Notify designated County contacts promptly of confirmed or suspected material security incidents.
- Assist with containment, eradication, recovery coordination, and post-incident analysis when requested.
- Provide monthly SOC activity reporting, including significant alerts, incidents, response actions, trends, and recommendations.

3.3 Security Engineering and Technical Support

- Provide cybersecurity engineering support to improve configurations, controls, architecture, and defensive capabilities.

- Review and assist with security configuration of firewalls, endpoints, servers, network devices, identity systems, email/security controls, backups, remote access, and other applicable technologies.
- Support vulnerability identification, prioritization, remediation tracking, and verification.
- Review patching and vulnerability management practices and identify material gaps.
- Support implementation or optimization of MFA, least privilege, secure remote access, endpoint protections, logging, backups, and other high-priority controls as applicable.
- Coordinate with the County and third-party technology providers so cybersecurity responsibilities are clearly assigned.
- Document material changes, remediation actions, and recommendations.

3.4 CPG Assessment

- Perform a facilitated CISA CPG assessment using the current applicable CISA CPG assessment methodology/tooling.
- Document the County's baseline status for each of the CPG goals.
- Identify gaps, risks, recommended actions, dependencies, responsible parties, evidence, and target dates.
- Provide an executive summary and a detailed technical report.
- Perform an annual reassessment before the end of the twelve-month service period and provide a comparison showing progress from the initial baseline.
- Update the CPG improvement roadmap based on assessment results and changes in the County's environment.

3.5 Information Security Policy Development / Update

- Review the County's existing information security policies, standards, procedures, and related documentation.
- Update existing policies or develop missing policies, in coordination with the County, necessary to support the CPG-aligned cybersecurity program.
- At a minimum, evaluate policies covering acceptable use, access control, password/credential security, MFA, remote access, incident response, backup/recovery, vulnerability/patch management, logging/monitoring, data protection, vendor/third-party risk, asset management, security awareness, and cybersecurity governance.
- Provide policies in editable electronic format and identify recommended approval/adoption actions for the County.
- Maintain a policy change log and annual review schedule.

3.6 Disaster Recovery / Incident Response Plan Update and Tabletop Exercise

- Review and update the County's Disaster Recovery and Incident Response plans or develop equivalent plans where absent.
- Establish clear roles, responsibilities, notification/escalation procedures, communications procedures, recovery priorities, and coordination requirements.
- Include ransomware, business email compromise, unauthorized access, malware, data loss, and other reasonably foreseeable cyber incidents.
- Conduct at least one tabletop exercise during the twelve-month term.
- Provide an after-action report identifying strengths, weaknesses, corrective actions, responsible parties, and target completion dates.
- Assist the County in maintaining the plans after the exercise.

3.7 Recurring Security Optimization Checks

Frequency	Minimum Activities
Daily	Review security alerts/incidents; review critical monitoring exceptions; identify urgent vulnerabilities or failed controls; escalate material issues; verify critical security services are functioning.
Weekly	Review vulnerability/patch status; endpoint/security-control health; privileged access/security events; backup/security exceptions; outstanding high-risk findings; tuning opportunities.
Monthly	vCISO review; CPG progress update; risk register update; security metrics; policy/action tracking; vulnerability trends; access/security review; management report.
Quarterly	Formal security posture review; CPG roadmap review; control effectiveness review; incident response readiness review; architecture/security engineering review; executive briefing; priorities for next quarter.

3.8 Incident Response Support

- Provide a documented incident intake and escalation process.
- Provide access to qualified incident response personnel during the contract term.
- Assist County personnel with evidence preservation, containment, remediation, recovery, communications, and lessons learned as appropriate.
- Clearly state in the proposal any limitations, exclusions, billable incident-response rates, or services not included in the base fee. No additional charge may be incurred without prior written authorization by the County.

4. REQUIRED DELIVERABLES AND PERFORMANCE STANDARDS

Deliverable	Minimum Requirement	Due/Timing
Kickoff & Environment Review	Kickoff meeting, points of contact, access requirements, service plan, technology inventory review.	Within 15 days of Notice to Proceed
Initial CPG Assessment	Facilitated assessment covering all applicable CPG goals; baseline report and gap analysis.	Within 60 days
Cybersecurity Improvement Roadmap	Prioritized remediation plan with County, priority, evidence, target date and status.	Within 60 days; update monthly
Information Security Policy Update	Updated policy and policy change log.	Within 90 days, then maintain
DR/IR Plan Update	Updated plans, roles, procedures, contacts and recovery priorities.	Within 120 days
Tabletop Exercise	Exercise plus after-action report and corrective action plan.	During contract term
Monthly vCISO Report	Executive summary, metrics, risk register, incidents, CPG progress and recommendations.	Monthly
SOC Report	Monitoring/alert/incident summary and trends.	Monthly
Quarterly Review	Formal posture review and executive briefing.	Quarterly
Annual CPG Assessment	Repeat assessment and year-over-year comparison.	Before contract expiration
Closeout Report	Final status of CPG goals, open risks, recommendations and transition information.	Within 15 days of term end

4.1 Service-Level Expectations

- The Contractor shall provide a primary account representative and a primary technical escalation contact.
- Critical security findings shall be escalated to the County Administrator without unreasonable delay.
- The Contractor shall maintain secure records of alerts, incidents, assessments, reports, recommendations, and completed remediation activities.
- Routine County requests shall receive an acknowledgement within one business day unless the proposal offers a shorter response commitment.
- Proposals shall state specific response and escalation commitments for Critical, High, Moderate, and Low severity events.

5. CISA CPG 2.0 ALIGNMENT AND GOAL COMPLIANCE

The County's grant application identifies full attention to all applicable CISA CPG goals. The Contractor shall therefore treat the CPGs as a core performance requirement rather than as a one-time assessment. The Contractor shall establish a baseline, identify gaps, recommend and support corrective actions, collect evidence, measure progress, and repeat the assessment annually.

Because CISA periodically revises its CPG materials, the Contractor shall use the current applicable CISA CPG assessment materials in effect at the time the assessment is performed. If a CPG is revised, renumbered, consolidated, or otherwise changed, the Contractor shall explain the mapping in the CPG Compliance Matrix.

- The initial assessment shall establish a documented baseline for every applicable goal.
- Every goal shall be classified as Met, Partially Met, Not Met, or Not Applicable, with a written explanation.
- Every gap shall have a recommended action, priority, responsible party, target date, and status.
- Not Applicable determinations shall be supported by a written rationale.
- The Contractor shall maintain the CPG Compliance Matrix throughout the contract.
- The annual assessment shall document measurable progress from the initial baseline.
- The Contractor shall identify actions requiring County policy decisions, technology purchases, configuration changes, staffing, training, or future funding.

6. COUNTY ENVIRONMENT AND COORDINATION

The County will identify authorized personnel and existing technology providers with whom the Contractor must coordinate. The Contractor shall not assume that it is replacing the County's existing IT functions unless specifically authorized. This solicitation is not meant to entertain the idea that the County will replace existing network infrastructure (firewalls, switches, backup devices, etc.,), change the network topology or acquire new network infrastructure devices as part of this contract, to meet an offering vendor’s requirements to perform services under this solicitation

- County will provide reasonable access to systems, documentation, personnel, and information necessary to perform the work, subject to security controls.
- Contractor shall use least-privilege access and shall not retain administrative access longer than necessary.
- Contractor shall coordinate all production-impacting changes with the County Administrator.
- Contractor shall not intentionally disable, bypass, or materially alter County security controls without documented authorization.
- Contractor shall maintain confidentiality of County information and shall use County data only for authorized contract purposes.
- Any subcontractor requiring access to County systems must be disclosed and approved in advance.

7. VENDOR MINIMUM QUALIFICATIONS

- At least five (5) years of demonstrated experience providing managed cybersecurity, vCISO, SOC, security engineering, or substantially similar services.
- Demonstrated experience serving governmental, public-sector, healthcare, financial, or other organizations with heightened security and compliance requirements.
- Demonstrated ability to perform or facilitate CISA CPG assessments and translate assessment findings into an actionable remediation program.
- Qualified personnel with appropriate cybersecurity experience and certifications. Proposers shall identify relevant certifications such as CISSP, CISM, CISA, GIAC, Security+, or equivalent credentials held by proposed personnel.
- Ability to provide documented incident response and escalation procedures.
- Ability to maintain secure handling of County information and administrative credentials.
- At least three (3) client references for substantially similar managed cybersecurity services.

8. PROPOSAL REQUIREMENTS

Proposals shall be organized in the following order:

1. Cover Letter – identify proposer, address, contact person, telephone, email, and authorized representative.
2. Executive Summary – concise description of the proposed solution and why it satisfies the RFP.
3. Company Qualifications – history, ownership, years in business, relevant public-sector experience, and organizational structure.
4. Proposed Team – identify vCISO, SOC leadership, security engineers, incident response personnel, and backups; include qualifications and certifications.
5. Technical Approach – describe monitoring, SOC, vCISO, security engineering, assessment, policy, DR/IR, tabletop, and recurring optimization approach.
6. CPG Approach – describe how all CPG goals will be assessed, tracked, evidenced, remediated, and reported.
7. Service Levels – provide response times, escalation model, monitoring hours, incident support, and service availability.
8. Implementation Plan – provide a 12-month schedule and first-90-day plan.
9. Deliverables – identify all deliverables included in the base price.
10. Security & Privacy – describe access control, data protection, logging, credential management, subcontractor controls, and incident notification.
11. References – at least three comparable client references.
12. Exceptions – clearly identify every requested RFP term to which the proposer takes exception.
13. Price Proposal – complete Appendix A.
14. Certifications – complete Appendix C.

9. PRICING REQUIREMENTS

The County will evaluate the completeness and reasonableness of proposed pricing in relation to the required scope.

Proposers shall provide:

- A firm total price for the full twelve-month base term.
- Monthly equivalent price for budgeting and payment purposes.
- A line-item description of any optional services, if offered. Optional services shall not be considered part of the base award unless expressly authorized.
- All recurring licensing, platform, SOC, reporting, assessment, and support costs necessary to deliver the proposed base service.

- Any one-time implementation or onboarding costs.
- Hourly rates for extraordinary services that may be requested outside the base scope, clearly separated from the base price.
- Identification of any third-party pass-through costs.

10. PROPOSAL EVALUATION AND SELECTION

Proposals will be evaluated by the County in accordance with applicable federal grant procurement requirements, County procurement procedures, and this RFP. The County may use a committee or designated evaluation team to review and score responsive proposals and may request clarification, conduct interviews, or request demonstrations.

Evaluation Criterion	Points
Technical approach and understanding of County objectives	25
CPG goal methodology, assessment, roadmap and measurable deliverables	20
Qualifications and relevant experience of firm and proposed team	20
SOC, vCISO, security engineering, incident response and service-level capabilities	15
Implementation plan, reporting and coordination	10
Price / cost reasonableness	10
TOTAL	100

The point allocations are intended to provide a transparent evaluation framework. The County may determine a proposal non-responsive if it fails to meet material mandatory requirements. The County will consider price/cost as required by applicable federal procurement standards and will not award solely on the basis of lowest price where the RFP requires the best professional and managed cybersecurity services.

11. CONTRACT TERMS AND CONDITIONS

- Contract Term – Twelve (12) months from the effective date or Notice to Proceed, as stated in the executed agreement.
- Funding – This project is funded in whole or in part through a cybersecurity grant. Expenditures must be allowable, allocable, reasonable, and consistent with the approved grant scope.
- Payment – Unless otherwise agreed in the final contract, the County anticipates monthly invoicing following satisfactory performance and acceptance of required services.
- Change Control – Material changes to scope, price, systems, or production configuration require written authorization.
- Ownership – Reports, assessments, policies, plans, matrices, documentation, and other work product specifically created for the County under this contract shall be provided to and usable by the County, subject to Contractor pre-existing intellectual property and applicable law.
- Confidentiality – Contractor shall protect County information and shall not disclose or use it except as authorized.
- Security Incident – Contractor shall notify the County promptly of any actual or suspected compromise involving County systems, credentials, data, or Contractor systems used to provide the services.
- Insurance – Contractor shall maintain insurance required by the County and applicable law, including commercially reasonable cyber liability/professional liability coverage appropriate to the services.
- Indemnification – As required by the final contract and applicable Mississippi law.
- Subcontracting – No material subcontractor may access County systems or information without prior written County approval.

- Termination – The County may terminate the contract for cause and, to the extent permitted by applicable law and grant terms, for convenience upon written notice.
- Audit/Records – Contractor shall maintain records necessary to substantiate performance and payment and make them available as required by applicable federal, state, and County requirements.
- Public Records – Contractor acknowledges that records associated with the contract may be subject to Mississippi public-records requirements, subject to applicable exemptions and protections.
- No Guaranteed Renewal – Any continuation beyond the initial twelve-month term must be separately authorized and must comply with grant funding and procurement requirements.

12. FEDERAL GRANT AND PROCUREMENT REQUIREMENTS

Because this procurement uses federal grant funds, the Contractor shall comply with applicable federal requirements incorporated into the County's award and contract. The County's solicitation and resulting contract are subject to 2 CFR Part 200, including applicable procurement standards in Subpart D, and the specific terms and conditions of the County's grant award and Mississippi Office of Homeland Security requirements.

- Contractor shall be eligible to receive federal funds and shall not be suspended or debarred from participation in federal awards.
- Contractor shall provide its legal name, tax identification information, and other information required for grant reporting or verification.
- Contractor shall comply with applicable federal conflict-of-interest, organizational conflict, and standards-of-conduct requirements.
- Contractor shall comply with applicable affirmative steps concerning minority businesses, women's business enterprises, and labor surplus area firms.
- Contractor shall comply with applicable federal restrictions concerning prohibited telecommunications and video surveillance equipment or services.
- Contractor shall comply with applicable lobbying restrictions and certifications.
- Contractor shall comply with applicable record-retention, audit, monitoring, and access requirements.
- Contractor shall flow down applicable federal requirements to approved subcontractors when required.
- Nothing in this RFP authorizes an expenditure that is not allowable under the County's specific grant award. If a proposed service is not clearly allowable, the County may exclude it from the award.

13. PROPOSAL FORMS AND CERTIFICATIONS

The following forms are included as appendices and shall be completed and returned with the proposal. Failure to submit required forms may result in a proposal being deemed non-responsive.

APPENDIX A – PRICE PROPOSAL FORM

MANAGED CYBERSECURITY SERVICES

Pricing Item	Proposer Price
One-time implementation/onboarding	$_____
Managed cybersecurity services – Month 1	$_____
Managed cybersecurity services – Months 2–12 (monthly)	$_____
Total twelve-month base contract price	**$**_____
Optional services (identify separately)	$_____
Extraordinary/after-hours hourly rate, if applicable	$_____

The undersigned certifies that the above price includes all services required by the RFP unless specifically identified as an exclusion or optional service.

Firm Name: _____

Authorized Representative: _____

Title: _____

Signature: _____

Date: _____

APPENDIX B – CPG COMPLIANCE MATRIX

The proposer shall provide a completed matrix in substantially the following format. The matrix shall identify the CPG goals and shall map each goal to the proposed services, evidence, measurement method, and planned action. The proposer may attach additional pages.

CPG Goal / Current CISA Designation	Baseline Method	Required/Proposed Action	Evidence / Metric	Target Timing	Responsible Party
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					
28					
29					
30					
31					
32					
33					
34					
35					
36					
37					
38					

APPENDIX C – REQUIRED VENDOR CERTIFICATIONS

CERTIFICATION OF NON-COLLUSION

The undersigned certifies that the proposal has been prepared independently and without collusion, consultation, communication, or agreement with any other proposer concerning price, terms, or conditions for the purpose of restricting competition.

Proposer: _____

Authorized Signature: _____

Printed Name/Title: _____

Date: _____

CERTIFICATION REGARDING SUSPENSION AND DEBARMENT

The undersigned certifies that the proposer and its principals are not suspended, debarred, or otherwise excluded from participation in federal awards, except as disclosed in writing with the proposal.

Proposer: _____

Authorized Signature: _____

Printed Name/Title: _____

Date: _____

CONFLICT OF INTEREST

The undersigned certifies that it has disclosed any actual, potential, or apparent conflict of interest involving the County, County officials/employees, the grant, or the procurement, and will promptly disclose any conflict arising during the contract.

Proposer: _____

Authorized Signature: _____

Printed Name/Title: _____

Date: _____

FEDERAL FUNDING COMPLIANCE

The undersigned agrees to comply with applicable federal grant requirements incorporated into the contract, including applicable requirements of 2 CFR Part 200 and the County's grant award.

Proposer: _____

Authorized Signature: _____

Printed Name/Title: _____

Date: _____

SUBCONTRACTORS

The undersigned has identified all known subcontractors who may participate in the services and will obtain County approval before granting any subcontractor access to County systems or information.

Proposer: _____

Authorized Signature: _____

Printed Name/Title: _____

Date: _____

TRUTH AND ACCURACY

The undersigned certifies that the information contained in the proposal is true and correct to the best of the signer's knowledge and that the signer is authorized to bind the proposer.

Proposer: _____

Authorized Signature: _____

Printed Name/Title: _____

Date: _____

APPENDIX D – SAMPLE SCOPE / DELIVERABLES SCHEDULE

Period	Primary Activities / Deliverables
Days 1–15	Kickoff; contacts; access; environment review; service plan; baseline documentation request.
Days 16–30	Security architecture review; monitoring/SOC onboarding; initial risk register; preliminary findings.
Days 31–60	Initial CPG assessment; 38-goal baseline; gap analysis; cybersecurity improvement roadmap.
Days 61–90	Policy review/update; DR/IR review/update; remediation support; management briefing.
Quarter 2	Optimization; vulnerability and control reviews; policy adoption support; tabletop preparation.
Quarter 3	Tabletop exercise; after-action report; remediation tracking; quarterly posture review.
Quarter 4	Annual CPG reassessment; year-over-year comparison; final roadmap; closeout report.
Every Month	vCISO meeting/report; SOC report; risk register; CPG tracking; security recommendations.
Daily/Weekly	Monitoring, alert review, security-control health, vulnerability/patch review and escalation as applicable.

APPENDIX E – PROPOSAL CHECKLIST

- Cover Letter
- Executive Summary
- Company Qualifications
- Proposed Personnel and Certifications
- Technical Approach
- CPG Goal Compliance Matrix
- Service Levels and Incident Response
- Implementation Schedule
- References
- Price Proposal Form
- Required Certifications
- Exceptions/Deviations Statement
- Any attachments or supporting documentation