

CARLYNTON SCHOOL DISTRICT

REQUEST FOR PROPOSALS

Independent Cybersecurity Risk Assessment and Penetration Testing Services

435 Kings Highway • Carnegie, Pennsylvania 15106

RFP Number	2026-001
Issue Date	October 5, 2026
Questions Due	October 19, 2026
Proposal Due	November 11, 2026
Anticipated Award	December 8, 2026
District Contact	Dr. Jeff Taylor, Assistant Superintendent jtaylor@carlynton.net 412-429-2500 ext)1113

CONFIDENTIALITY NOTICE

The successful proposer will receive security-sensitive technical information only after appropriate authorization and confidentiality protections are in place.

Table of Contents

1. Purpose	3
2. District Background	3
3. Project Objectives	3
4. Required Cybersecurity Frameworks	4
5. Scope of Services	4
6. Rules of Engagement	8
7. Critical Vulnerability Notification	8
8. Required Deliverables	8
9. Vendor Independence and Conflict of Interest	10
10. Minimum Vendor Qualifications	10
11. Personnel Qualifications	10
12. References	11
13. Data Security and Confidentiality	11
14. Use of Artificial Intelligence and Third-Party Services	11
15. Cyber Insurance and Professional Liability	12
16. Subcontractors	12
17. Proposal Format	12
18. Pricing Schedule	13
19. Proposed Project Timeline	14
20. Evaluation Criteria	14
21. Vendor Interview / Demonstration	15
22. Proposal Questions	15
23. Proposal Submission	15
24. Reservation of Rights	16
25. Public Records and Confidentiality of Proposals	16
26. Contract Requirements	16
27. Ownership of Deliverables	17
28. Proposer Certification	17
Appendix A – Technical Scope Checklist	18
Appendix B – Reference Form	20
Appendix C – Conflict / Independence Disclosure	21
Appendix D – Proposal Score Sheet	22
Appendix E – Proposal Submission & Signature Page	23
Appendix F – District Award / Approval Signature Page	24

1. PURPOSE

The Carlynton School District (“District”) is requesting proposals from qualified, independent cybersecurity firms to conduct a comprehensive cybersecurity risk assessment, vulnerability assessment, and penetration test of the District’s information technology environment.

The purpose of this engagement is to independently evaluate the District’s current cybersecurity posture; identify technical, administrative, and operational vulnerabilities; evaluate the District’s preparedness to prevent, detect, respond to, and recover from cybersecurity incidents; and develop a prioritized remediation roadmap that includes, but is not limited to:

- Technical findings that can be acted upon by District technology personnel,
- Executive-level findings that can be used by District administration and the Board of School Directors for cybersecurity planning, budgeting, risk management, and policy development.

This RFP is intended to procure an independent cybersecurity assessment. It is not primarily a solicitation for managed IT services, cybersecurity products, hardware, software, or ongoing security operations.

2. DISTRICT BACKGROUND

Carlynton School District is a Pennsylvania public school district located in Allegheny County serving the communities of Carnegie, Crafton, and Rosslyn Farms.

- Carnegie Elementary School – Grades K–6
- Crafton Elementary School – Grades K–6
- Carlynton Junior-Senior High School – Grades 7–12

The District serves approximately 1,300 students in addition to faculty, administrators, support personnel, and other authorized technology users.

The District maintains a technology environment supporting instructional, administrative, financial, student-information, communications, security, and operational systems. Additional technical information necessary for the assessment may be provided to the selected vendor following execution of appropriate confidentiality and data-security agreements.

3. PROJECT OBJECTIVES

- a) Establish an independent baseline of the District’s cybersecurity posture.
- b) Identify vulnerabilities that could permit unauthorized access, ransomware, data exfiltration, privilege escalation, lateral movement, or disruption of District operations.
- c) Evaluate cybersecurity governance, policies, procedures, and administrative controls.
- d) Assess internal and external technology vulnerabilities.
- e) Evaluate identity and access-management practices.
- f) Evaluate the security of cloud and collaboration environments.
- g) Evaluate network architecture and segmentation.
- h) Assess backup, disaster recovery, and ransomware resilience.
- i) Evaluate incident-response preparedness.
- j) Identify risks associated with privileged accounts and administrative access.
- k) Evaluate cybersecurity practices against recognized cybersecurity frameworks.
- l) Prioritize vulnerabilities according to risk and operational impact.
- m) Develop a practical remediation roadmap.
- n) Provide District leadership with an executive-level assessment of organizational cyber risk.
- o) Validate remediation efforts through follow-up testing.

4. REQUIRED CYBERSECURITY FRAMEWORKS

At minimum, the assessment shall consider applicable components of:

- NIST Cybersecurity Framework (CSF) 2.0;
- CIS Critical Security Controls;
- applicable CISA K–12 cybersecurity guidance;
- applicable Pennsylvania school cybersecurity requirements and guidance;
- FERPA-related information-security considerations; and
- generally accepted cybersecurity and penetration-testing standards.

The vendor shall identify the methodology and standards used in its proposal.

5. SCOPE OF SERVICES

A. Cybersecurity Governance and Risk Assessment

Review the District’s cybersecurity governance structure and administrative controls, including, where applicable:

- cybersecurity policies and administrative procedures;
- roles and responsibilities;
- risk-management processes;
- acceptable-use policies;
- account-management procedures;
- privileged-access management;
- password and authentication practices;
- multifactor authentication;
- onboarding and offboarding procedures;
- cybersecurity awareness training;
- incident reporting;
- vendor and third-party risk management;
- data governance;
- cyber insurance requirements;
- business continuity;
- disaster recovery; and
- incident-response planning.

The assessment shall identify gaps between existing District practices and recognized cybersecurity standards.

B. External Vulnerability Assessment

Conduct a comprehensive vulnerability assessment of authorized District internet-facing assets. Testing should identify, as applicable:

- exposed systems and services;
- obsolete or unsupported systems;
- unpatched vulnerabilities;
- misconfigurations;
- unnecessary services;
- exposed management interfaces;
- certificate/security issues;
- DNS-related vulnerabilities;
- email-security configuration issues;

- remote-access vulnerabilities; and
- other externally exploitable conditions.

C. External Penetration Testing

Conduct controlled external penetration testing designed to determine whether identified vulnerabilities can be exploited by an unauthorized external actor.

The vendor shall use accepted penetration-testing methodologies and shall take appropriate measures to avoid interruption of District operations. Testing shall not include destructive activities, denial-of-service testing, or other activities that could materially disrupt District operations unless separately authorized in writing.

D. Internal Vulnerability Assessment and Penetration Testing

Conduct internal testing from an authorized location within the District environment. Testing should evaluate:

- network segmentation;
- lateral movement opportunities;
- privilege escalation;
- credential exposure;
- insecure protocols;
- unnecessary services;
- administrative shares;
- patching vulnerabilities;
- endpoint exposure;
- internal access controls; and
- opportunities through which an attacker could move from a compromised endpoint to higher-value systems.

The District is particularly interested in understanding the potential consequences of a scenario in which a standard staff or student endpoint has been compromised.

E. Active Directory / Identity Infrastructure Assessment

Evaluate applicable identity-management infrastructure, including Active Directory. The assessment should address:

- privileged accounts;
- excessive permissions;
- dormant accounts;
- service accounts;
- legacy authentication;
- password policies;
- MFA deployment;
- conditional-access policies;
- administrative roles;
- privilege escalation pathways;
- credential exposure; and
- other identity-related vulnerabilities.

F. Microsoft 365 / Google Workspace for Education - Cloud Security Assessment

Evaluate the District's applicable Microsoft 365/Google Workspace for Education cloud security configurations. Review should include, as applicable:

- administrator roles;
- MFA;

- conditional access;
- external sharing;
- email-security controls;
- malicious forwarding rules;
- legacy authentication;
- guest accounts;
- application permissions;
- audit logging;
- security alerts;
- account compromise protections; and
- data-access controls.

If other major cloud platforms are identified during the engagement, the vendor shall advise the District of significant cybersecurity risks associated with those environments.

G. Network Architecture and Segmentation Review

Evaluate network architecture from a cybersecurity perspective, including:

- firewall configuration;
- VLAN/network segmentation;
- student/staff/administrative separation;
- server networks;
- wireless networks;
- guest access;
- Internet of Things (IoT) devices;
- printers;
- security systems;
- building systems;
- remote access; and
- other network-connected infrastructure.

The assessment shall specifically identify conditions that could facilitate lateral movement following compromise of a user device.

H. Backup, Recovery and Ransomware Resilience

Evaluate the District's ability to recover from ransomware or other destructive cybersecurity incidents. Review should address:

- backup architecture;
- backup frequency;
- backup isolation;
- immutable/offline backups;
- administrative access;
- backup monitoring;
- restoration testing;
- recovery priorities;
- recovery-time objectives;
- recovery-point objectives; and
- protection of backup systems from compromised administrator credentials.

The vendor should assess whether a successful attack on the District's primary network could reasonably compromise its recovery systems.

I. Incident-Response Plan Review

Review the District's cybersecurity incident-response procedures. The vendor shall evaluate:

- roles and responsibilities;
- internal notification procedures;
- escalation;
- cyber-insurance notification;
- law-enforcement/CISA notification;
- legal counsel involvement;
- communications;
- evidence preservation;
- system isolation;
- restoration;
- data-breach evaluation; and
- post-incident activities.

Recommendations shall be provided for identified deficiencies.

J. Cybersecurity Tabletop Exercise

Conduct at least one cybersecurity tabletop exercise with appropriate District personnel. The exercise should simulate a realistic K–12 cybersecurity event such as ransomware, compromised administrator credentials, data exfiltration, or widespread system disruption. The exercise should include appropriate representatives from:

- District administration;
- technology;
- communications;
- business operations;
- student services or other relevant departments; and
- other personnel designated by the District.

The vendor shall provide an after-action summary identifying lessons learned and recommended improvements.

6. RULES OF ENGAGEMENT

Prior to penetration testing, the successful vendor and District shall establish written Rules of Engagement.

- authorized systems;
- excluded systems;
- testing dates and times;
- authorized testing methods;
- emergency contacts;
- escalation procedures;
- procedures for critical vulnerability notification;
- prohibited testing activities;
- procedures for protecting collected information; and
- procedures for terminating testing if an operational risk is identified.

No penetration testing shall begin without written District authorization.

7. CRITICAL VULNERABILITY NOTIFICATION

The successful vendor shall immediately notify designated District officials upon discovering a vulnerability that presents an imminent or critical risk to District systems, information, or operations.

Independent Cybersecurity Risk Assessment and Penetration Testing Services

The vendor shall not wait until issuance of the final report to disclose critical findings. A secure communication method shall be established for transmitting sensitive findings.

8. REQUIRED DELIVERABLES

A. Technical Cybersecurity Assessment Report

A confidential technical report containing:

- testing methodology;
- systems/categories evaluated;
- identified vulnerabilities;
- evidence supporting findings;
- vulnerability severity;
- likelihood of exploitation;
- potential operational impact;
- affected assets;
- recommended remediation;
- technical references; and
- prioritization.

Findings should be categorized at minimum as Critical, High, Medium, Low, and Informational. Where appropriate, findings should include CVSS scoring or another recognized risk-scoring methodology.

B. Executive Cybersecurity Report

A separate executive report suitable for District leadership shall:

- summarize overall cybersecurity posture;
- identify major organizational risks;
- identify critical/high-priority deficiencies;
- explain potential operational consequences;
- identify significant strengths;
- summarize recommended investments; and
- provide a prioritized improvement roadmap.

The executive report shall avoid unnecessary disclosure of exploitable technical details.

C. Cybersecurity Maturity Assessment

Provide an assessment of the District's maturity against NIST CSF 2.0 and/or CIS Controls. The assessment should identify:

- current maturity;
- significant gaps;
- target state; and
- recommended actions.

D. Prioritized Remediation Roadmap

Provide a remediation roadmap organized, at minimum, into:

- Immediate: 0–30 days
- Near Term: 31–90 days
- Intermediate: 3–12 months
- Strategic: 1–3 years

Recommendations should distinguish among configuration/process changes achievable with existing resources; investments requiring new software or services; infrastructure investments; staffing or professional-service needs; and policy/governance improvements.

E. Executive Presentation

Present the findings to District administration and other personnel designated by the District.

The District may also request a presentation or executive session briefing for the Board of School Directors, subject to applicable Pennsylvania law and the need to protect confidential cybersecurity information.

F. Remediation Retest

Approximately 90–180 days following delivery of the final report, or at another mutually agreed time, the vendor shall retest Critical and High findings that the District reports as remediated. The vendor shall provide written validation indicating whether each finding has been:

- Remediated;
- Partially Remediated; or
- Not Remediated.

Pricing for this retest shall be included in the base proposal.

9. VENDOR INDEPENDENCE AND CONFLICT OF INTEREST

The District seeks an independent assessment. Proposers shall disclose:

- Any current or previous business relationship with Carlynton School District.
- Any products or services currently provided to the District.
- Any products, hardware, software, subscriptions, managed services, or consulting services the proposer may recommend or seek to sell to the District as a result of this assessment.
- Any financial relationships with manufacturers or cybersecurity vendors whose products may be recommended.
- Any other actual or potential conflict of interest.

The District reserves the right to consider vendor independence when evaluating proposals. The successful vendor shall not condition findings or recommendations upon the District's purchase of products or services from the vendor.

10. MINIMUM VENDOR QUALIFICATIONS

Proposers should demonstrate:

- substantial professional cybersecurity experience;
- penetration-testing experience;
- experience conducting cybersecurity assessments;
- experience with Microsoft environments;
- experience with K–12 educational organizations;
- familiarity with Pennsylvania public-school environments;
- familiarity with FERPA and student-data security;
- appropriate professional liability and cyber liability insurance; and
- qualified cybersecurity professionals assigned to the engagement.

Preference may be given to firms demonstrating successful cybersecurity engagements with Pennsylvania public school districts, intermediate units, governmental agencies, or comparable organizations.

11. PERSONNEL QUALIFICATIONS

The proposal shall identify all key personnel anticipated to work on the project and provide relevant credentials. Relevant certifications may include, but are not limited to:

- CISSP;
- OSCP;
- GIAC certifications;
- CISA;
- CISM;
- CRISC;
- CEH; or
- comparable industry-recognized credentials.

Certifications alone will not substitute for demonstrated penetration-testing and K–12 cybersecurity experience. The District reserves the right to approve key personnel assigned to the project.

12. REFERENCES

Provide at least three references for comparable cybersecurity assessment or penetration-testing engagements. Preference is given to Pennsylvania K–12 public school entities. For each reference provide:

- organization;
- contact name/title;
- telephone number;
- email;
- approximate engagement date;
- services performed; and
- approximate size/scope of the organization.

13. DATA SECURITY AND CONFIDENTIALITY

Information obtained through this engagement shall be considered confidential and used solely for purposes of performing contracted services. The successful vendor shall:

- limit access to District information to authorized personnel;
- use secure encrypted methods for storage and transmission;
- not use District information for marketing or unrelated purposes;
- not disclose vulnerabilities to third parties without written authorization;
- notify the District immediately of any unauthorized disclosure;
- comply with applicable federal and Pennsylvania privacy/security requirements; and
- securely destroy or return District information upon completion of the engagement according to mutually agreed requirements.

The District may require execution of additional confidentiality, nondisclosure, data-security, and/or data-processing agreements.

14. USE OF ARTIFICIAL INTELLIGENCE AND THIRD-PARTY SERVICES

The proposer shall disclose whether generative artificial intelligence systems, cloud-based analysis platforms, subcontractors, offshore resources, or other third-party services will receive, process, retain, or have access to District confidential information, credentials, vulnerability information, network information, student information, employee information, or other protected information.

District confidential information shall not be entered into publicly available generative AI systems. Any use of third-party systems involving District confidential information must be expressly authorized by the District and appropriately secured.

15. CYBER INSURANCE AND PROFESSIONAL LIABILITY

The successful vendor shall maintain insurance appropriate for the engagement, including, at minimum, professional liability/errors and omissions and cybersecurity/privacy liability coverage. The proposer shall provide:

- coverage types;
- coverage limits;
- insurance carrier; and
- evidence of coverage upon request.

The District reserves the right to establish minimum insurance requirements prior to contract execution.

16. SUBCONTRACTORS

All subcontractors anticipated to perform work under the engagement must be disclosed in the proposal. The proposer shall identify:

- subcontractor;
- services to be performed;
- location from which services will be performed; and
- access the subcontractor will have to District systems or information.

No undisclosed subcontractor may access District systems or confidential information without prior written District authorization.

17. PROPOSAL FORMAT

Proposal Section	Required Content
Section 1 – Executive Summary	Overview of the proposed approach.
Section 2 – Company Qualifications	Company background and relevant cybersecurity experience.
Section 3 – Pennsylvania K–12 Experience	Description of relevant public-school cybersecurity engagements.
Section 4 – Proposed Methodology	Detailed explanation of how the scope of services will be completed.
Section 5 – Project Team	Personnel, roles, qualifications, certifications, and experience.
Section 6 – Project Schedule	Proposed timeline from kickoff through final report and remediation retesting.
Section 7 – Deliverables	Description/sample structure of proposed deliverables.
Section 8 – References	Minimum of three references.
Section 9 – Independence and Conflicts	Required disclosures described in this RFP.
Section 10 – Data Security	Description of methods used to secure District information.
Section 11 – Exceptions	Identification of any exceptions to the RFP requirements.
Section 12 – Pricing	Completed pricing schedule.

18. PRICING SCHEDULE

Proposers shall provide fixed pricing wherever possible. The total fixed project cost should represent the District's maximum cost for completing the required scope unless the District subsequently authorizes additional services.

Service	Cost
Cybersecurity governance/risk assessment	\$_____
External vulnerability assessment	\$_____
External penetration testing	\$_____
Internal vulnerability/penetration testing	\$_____
Active Directory assessment	\$_____
Microsoft 365/Google Workspace for Education - cloud security assessments	\$_____
Network architecture/segmentation assessment	\$_____
Backup/ransomware resilience assessment	\$_____
Incident-response review	\$_____
Cybersecurity tabletop exercise	\$_____
Executive and technical reports	\$_____
Executive presentation	\$_____
90-180 day remediation retest	\$_____
TOTAL FIXED PROJECT COST	\$_____

The proposer shall clearly identify all travel, lodging, administrative, licensing, scanning, reporting, or other expenses.

Optional Services

Optional Service	Cost
Annual external vulnerability scanning	\$_____
Annual penetration testing	\$_____
Additional tabletop exercise	\$_____
Additional remediation testing	\$_____
vCISO/advisory services	\$_____
Other: _____	\$_____

Optional services shall not be included in the base project price.

19. PROPOSED PROJECT TIMELINE

Milestone	Anticipated Date
RFP Issued	October 5, 2026
Vendor Questions Due	October 19, 2026
District Responses	November 2, 2026
Proposals Due	November 11, 2026
Vendor Interviews, if necessary	November 18-20, 2026
Recommendation to Board	December 4, 2026
Anticipated Board Approval	December 8, 2026
Project Kickoff	January 13, 2027
Testing Period	January 20, 2027 - February 10, 2027 (<i>tentative</i>)
Draft Report	March 10, 2026 (<i>tentative</i>)
Final Report	March 31, 2026 (<i>tentative</i>)
Remediation Retesting	Approximately 90–180 days following final report

The District reserves the right to modify this schedule.

20. EVALUATION CRITERIA

Evaluation Factor	Weight
Technical methodology and completeness of proposed scope	25%
K–12/Pennsylvania public-sector cybersecurity experience	20%
Qualifications and experience of assigned personnel	15%
Independence/objectivity	10%
Quality and usefulness of proposed deliverables	10%
Cost/value	15%
References/project management/timeline	5%
TOTAL	100%

The lowest-cost proposal will not necessarily be selected. The District reserves the right to interview finalists, request clarification, negotiate scope and pricing, and consider other relevant factors permitted by law.

21. VENDOR INTERVIEW / DEMONSTRATION

The District may invite selected proposers to an interview. Sales personnel should not substitute for technical personnel during finalist interviews.

Finalists may be asked to:

- explain their testing methodology;
- introduce personnel who will actually conduct the assessment;
- demonstrate the format of a sanitized sample report;
- explain how findings are prioritized;
- describe how critical vulnerabilities are communicated;
- explain their experience in K–12 environments; and
- discuss how vendor independence is maintained.

22. PROPOSAL QUESTIONS

All questions regarding this RFP shall be submitted in writing to:

Dr. Jeff Taylor, Assistant Superintendent
Carlynton School District | Email: jtaylor@carlynton.net

Please include “**RFP Questions**” in the Subject Line for all emails for proposal questions. Questions must be received by **2:00pm on October 19, 2026**. Responses that materially affect the RFP may be distributed to all known proposers.

23. PROPOSAL SUBMISSION

Proposals must be received by **2:00pm on November 11, 2026** to:

Printed Proposal Submissions: Carlynton School District, 435 Kings Highway, Carnegie, PA 15106 | Attn: Dr. Jeff Taylor – RFP Proposal

OR

Electronic Proposal Submissions: Email: jtaylor@carlynton.net. Please include “**RFP Proposal**” in the Subject Line of the email. The proposal should be attached as a PDF formatted document.

Late proposals may be rejected.

24. RESERVATION OF RIGHTS

To the extent permitted by applicable law, the Carlynton School District reserves the right to:

- reject any or all proposals;
- waive informalities or irregularities;
- request additional information;
- seek clarification;
- conduct interviews;
- negotiate with one or more proposers;
- modify the anticipated scope;
- cancel or reissue the RFP;
- verify references and representations;
- determine whether a proposer is responsible and qualified;
- select the proposal determined to provide the best overall value to the District; and
- make no award.

25. PUBLIC RECORDS AND CONFIDENTIALITY OF PROPOSALS

The District is subject to the Pennsylvania Right-to-Know Law.

Independent Cybersecurity Risk Assessment and Penetration Testing Services

- Proposers should clearly identify information they believe is confidential, proprietary, security-sensitive, or otherwise exempt from disclosure under applicable law.
- Designation of information as confidential by a proposer does not necessarily determine whether the information is exempt from disclosure.
- Because this engagement will involve information concerning cybersecurity vulnerabilities and information systems, the District will handle security-sensitive materials consistent with applicable law and District procedures.

26. CONTRACT REQUIREMENTS

The selected proposer will be required to enter into a written agreement acceptable to the District. The final agreement may address:

- scope;
- pricing;
- confidentiality;
- cybersecurity;
- data protection;
- insurance;
- indemnification;
- limitation of liability;
- ownership of work product;
- subcontractors;
- breach notification;
- records retention/destruction;
- termination;
- Pennsylvania law;
- background requirements where applicable; and
- other terms required by the District.

The District's RFP, successful proposal, written clarifications, and negotiated modifications may be incorporated into the final agreement.

27. OWNERSHIP OF DELIVERABLES

Final reports, assessments, remediation plans, presentations, and other District-specific deliverables produced under the engagement shall be provided to the District for its unrestricted internal governmental use, subject to any mutually agreed rights concerning the vendor's preexisting methodologies, tools, and intellectual property.

- The vendor shall not publicly disclose the District's results, vulnerabilities, security posture, or participation in the engagement without prior written authorization.

28. PROPOSER CERTIFICATION

By submitting a proposal, the proposer certifies that:

1. Information contained in the proposal is accurate to the best of its knowledge.
2. The proposer has disclosed known conflicts of interest.
3. Pricing includes all services necessary to perform the proposed scope except items expressly identified as optional or excluded.
4. The proposer will protect District confidential information.
5. The proposer will not conduct penetration testing beyond the scope expressly authorized by the District.
6. The proposer has the professional expertise and resources necessary to perform the engagement.

Independent Cybersecurity Risk Assessment and Penetration Testing Services

Company	
Authorized Representative	
Title	
Signature	
Date	

APPENDIX A – TECHNICAL SCOPE CHECKLIST

Proposers shall indicate whether each item is included in the base price.

Assessment Area	Included	Not Included	Comments
NIST CSF 2.0 assessment	☐	☐	
CIS Controls assessment	☐	☐	
External vulnerability scanning	☐	☐	
External penetration testing	☐	☐	
Internal vulnerability scanning	☐	☐	
Internal penetration testing	☐	☐	
Assumed-breach testing	☐	☐	
Active Directory assessment	☐	☐	
Microsoft 365/ Google Workspace for Education – cloud security assessment	☐	☐	
MFA/conditional-access review	☐	☐	
Privileged-account review	☐	☐	
Network segmentation review	☐	☐	
Firewall security review	☐	☐	
Wireless security review	☐	☐	
IoT/device segmentation review	☐	☐	
Backup/ransomware resilience	☐	☐	
Incident-response plan review	☐	☐	
Cybersecurity tabletop exercise	☐	☐	
Executive report	☐	☐	
Detailed technical report	☐	☐	
3-year remediation roadmap	☐	☐	
Executive presentation	☐	☐	
90–180 day retest	☐	☐	

APPENDIX B – REFERENCE FORM

Complete one form for each reference. Attach additional copies as needed.

Organization: _____

Type of Organization: _____

Approximate Users/Endpoints: _____

Services Performed: _____

Engagement Date: _____

Contact: _____

Title: _____

Telephone: _____

Email: _____

Reference Notes (District use):

APPENDIX C – CONFLICT / INDEPENDENCE DISCLOSURE

1. Does your company currently provide technology or cybersecurity products or services to Carlynton School District?

☐ Yes ☐ No

If yes, explain:

2. Does your company intend to recommend products or services from which it may financially benefit?

☐ Yes ☐ No

If yes, explain:

3. Does your company receive commissions, referral fees, reseller margins, or other compensation from technology vendors whose products could be recommended through this assessment?

☐ Yes ☐ No

If yes, identify the relationships:

4. Identify any other potential conflict of interest:

APPENDIX D – PROPOSAL SCORE SHEET

Vendor: _____

Category	Weight	Score
Technical methodology/scope	25	
PA K–12/public-sector experience	20	
Personnel qualifications	15	
Independence/objectivity	10	
Deliverables	10	
Cost/value	15	
References/timeline/project management	5	
TOTAL	100	

Evaluator: _____

Date: _____

Strengths:

Concerns:

Exceptions / Qualifications:

Overall Recommendation:

☐ Highly Recommended ☐ Recommended ☐ Consider ☐ Not Recommended

APPENDIX E – PROPOSAL SUBMISSION & SIGNATURE PAGE

This page should be completed and signed by an individual authorized to bind the proposer.

Legal Company Name: _____

DBA (if applicable): _____

Business Address: _____

City / State / ZIP: _____

Primary Contact: _____

Title: _____

Telephone: _____

Email: _____

Federal EIN (optional at proposal stage): _____

Acknowledgment

The undersigned certifies that the proposer has reviewed the RFP, including all appendices and issued addenda, and agrees that the proposal will remain valid for the period stated by the District or, if none is stated, for 90 days following the proposal due date.

Authorized Signature: _____

Printed Name: _____

Title: _____

Date: _____

APPENDIX F – DISTRICT AWARD / APPROVAL SIGNATURE PAGE

For District use following Board approval and completion of any required contract review.

Selected Vendor: _____

Approved Contract Amount: _____

Board Approval Date: _____

Board Motion / Resolution Reference: _____

Contract Effective Date: _____

CARLYNTON SCHOOL DISTRICT

Authorized District Representative: _____

Title: _____

Signature: _____

Date: _____

VENDOR ACCEPTANCE

Authorized Vendor Representative: _____

Title: _____

Signature: _____

Date: _____