Fountain • Fort Carson
SCHOOL DISTRICT EIGHT

Landon Finch
Director of Technology
425 W Alabama Ave, Fountain, CO 80817
719.382.1608
rfp@ffc8.org

March 3, 2026

Request For Proposals Network Penetration Testing & Hybrid Identity Risk Validation Assessment - 2026

DATE DUE: March 17, 2026 11:59 PM MST

---

1. Introduction

Fountain-Fort Carson School District 8 serves students and staff across multiple school and administrative sites within a centrally managed technology environment. The District seeks proposals from qualified cybersecurity firms to conduct a focused, time-boxed network penetration testing and hybrid identity risk validation engagement.

The District's environment includes:

- Single Active Directory forest
- Hybrid identity integration with cloud identity services (Entra ID)
- Microsoft 365
- Google Workspace
- Enterprise device management platforms
- On-premises servers and infrastructure
- Remote access and single sign-on solutions

Google Workspace identity configuration is explicitly out of scope for this engagement.

The District has completed prior external vulnerability scanning through a federal assessment program. Relevant findings will be provided to qualified vendors following execution of a Non-Disclosure Agreement (NDA) and completion of vendor vetting. These findings are

provided to enable validation and exploitation assessment — not to repeat broad external discovery scanning.

Detailed network documentation, addressing information, and relevant architecture details will be transmitted via secure methods designated by the District following NDA execution. Contact us at **rfp@ffc8.org** for the NDA document.

The purpose of this engagement is to provide validated visibility into high-impact, materially exploitable conditions within the defined scope, along with practical and prioritized remediation guidance. This is a focused validation exercise and not a comprehensive enterprise-wide assessment.

---

2. Purpose and Objectives

The objectives of this time-bound engagement are to:

- Identify and validate high-impact exploitable conditions within the defined scope
- Attempt to demonstrate at least one realistic, multi-stage attack path where feasible within the time constraint
- Assess privilege escalation risks accessible from a single internal foothold
- Identify obvious exposures affecting systems believed to contain student, personnel, or financial data
- Evaluate hybrid identity exposure reachable from the internal foothold (AD-to-cloud privilege paths)
- Provide prioritized and implementable remediation guidance appropriate to a K–12 operational environment

Within the internal testing component, vendors should prioritize identifying conditions where a standard user context can be leveraged to escalate into hybrid identity (Entra ID / M365) or reach systems believed to contain student or financial data. This transition — from internal foothold to privileged identity or sensitive data access — represents the highest-value outcome within this engagement scope.

If no materially exploitable multi-stage path is identified within the defined scope and time constraint, vendors must provide documented evidence of testing depth sufficient to support that conclusion. Absence of findings requires substantiation, not mere assertion.

SCOPE INTENT

This engagement is not intended to serve as a comprehensive enterprise-wide assessment. Vendors who propose equal coverage of all surface areas within five (5) person-days will be evaluated skeptically. Realistic prioritization and validation rigor within a defined focus area are valued over breadth of coverage.

3. Engagement Standards and Expectations

3.1 Risk Validation

The District prioritizes validated risk over volume of findings. Vendors must:

- Demonstrate manual validation practices beyond automated scanning
- Clearly distinguish validated exploitable risks from informational or lower-confidence observations
- Articulate business and instructional impact in terms meaningful to non-technical leadership
- Describe how framework alignment (e.g., NIST SP 800-115, PTES, MITRE ATT&CK) informs practical testing methodology — not merely cite frameworks

Automated scanning alone is insufficient. Findings based solely on tool output without manual validation explanation will receive reduced evaluation scores.

3.2 Adversary Realism

Testing should reflect realistic attacker behavior within the defined time constraints. Where feasible, vendors should attempt to demonstrate at least one multi-stage attack progression showing plausible attacker movement within the District's hybrid identity environment.

Exhaustive attack chain modeling is not expected within this scope. A single well-documented, validated attack path demonstrating realistic progression carries more evaluation weight than a high volume of isolated findings without contextual linkage.

3.3 Remediation Guidance

Recommendations must be practical and implementable within a K–12 environment with limited IT staffing. Vendors must:

- Clearly prioritize findings with structured sequencing
- Distinguish immediate risk-reduction steps from longer-term architectural improvements
- Identify operational dependencies or constraints where relevant
- Offer alternative risk-reduction options where full remediation is not immediately feasible

Remediation volume alone is not indicative of quality. The District values structured prioritization and feasibility over exhaustive recommendation lists.

3.4 Operational Stability

Testing must be conducted with safeguards appropriate to a live instructional environment. Vendors must demonstrate:

- Experience minimizing disruption to live school environments
- Lockout prevention controls for authentication-based testing
- Defined emergency stop procedures with named point of contact
- Secure handling of privileged credentials and authentication tokens

---

4. Scope of Services

The total engagement shall not exceed five (5) consultant person-days, inclusive of testing, reporting, QA, readouts, and consultation. Vendors must explicitly allocate person-days across phases in their proposals.

Anticipated Allocation Model

Phase	Focus	Estimated Person-days
External Validation	Manual validation & exploitation of prior federal findings	0.5
Internal Testing	Single foothold – lateral movement & privilege escalation	2–2.5
Identity Validation	AD & hybrid privilege exposure from foothold	0.75–1
Reporting & Readouts	Deliverables, combined briefing, consultation	1–1.5

4.1 External Validation

The District has previously conducted external vulnerability scanning through a federal assessment program. Vendors will be provided relevant findings following NDA execution.

This component is focused on:

- Manual validation of assessment-identified findings
- Safe exploitation attempts where appropriate

- Determination of real-world exploitability within the District's configuration
- Assessment of whether identified external findings provide a viable path toward internal systems

Broad external discovery scanning is not required and should not be priced into proposals. The prior assessment findings are provided as a baseline and do not require re-scoring. Vendors are expected to validate exploitability and contextual impact.

Limited additional surface review may be performed within the allocated 0.5 person-days at vendor discretion.

4.2 Internal Testing (Single Foothold)

Testing from one authorized internal device provided by the District. Focus areas include:

- Lateral movement opportunities within the accessible segment
- Privilege escalation paths from a standard user context
- Validation of at least one materially exploitable internal condition, where feasible

If no materially exploitable condition is identified, vendors must provide documented evidence of testing depth sufficient to support that conclusion.

4.3 Targeted Identity Risk Validation

A focused review of Active Directory privilege exposure and hybrid identity risk reachable from the internal foothold.

This component includes:

- Review of high-risk AD privileged group assignments
- Identification of obvious delegation or authentication misconfigurations
- Focused assessment of AD-to-cloud (Entra ID / M365) privilege exposure reachable from the foothold

Analysis is limited to privilege exposure reachable from the provided foothold and does not require enterprise-wide effective permission mapping or comprehensive identity architecture review. Group membership enumeration alone is insufficient.

OUT OF SCOPE

- Google Workspace identity configuration
- M365 security configuration beyond what is reachable from the internal foothold

- Enterprise-wide effective permission mapping
- Comprehensive identity architecture assessment

Vendors should not price or propose coverage of these areas.

4.4 Deliverables

The engagement must include:

- Executive summary suitable for non-technical leadership and school board
- Risk-ranked findings with validation explanation for critical and high findings
- Business impact articulation in operational and instructional terms
- Prioritized remediation list with short-term and longer-term sequencing
- One technical readout briefing session (minimum 90 minutes)
- Up to 2 hours of post-engagement consultation support

Technical findings may be presented concisely, provided that the primary attack path (where identified) is documented in sufficient detail for reproduction and remediation.

All deliverables become the sole property of the District.

---

5. Technical Approach and Methodology Requirements

Vendors must describe:

- Manual validation practices
- Explicit allocation of effort across phases (must not exceed 5 total person-days)
- How testing effort will be realistically prioritized within time constraints
- False positive reduction methods and QA process
- Senior versus junior analyst participation
- Operational safeguard integration

Proposed fees must be all-inclusive. This engagement is expected to be conducted remotely.

Separate optional retest pricing must be provided.

---

6. Rules of Engagement and Operational Safeguards

Vendors must describe:

- Testing windows and coordination process

- Lockout avoidance controls
- Emergency stop procedures and named escalation contacts
- Data handling and destruction policies
- Incident notification protocol (within 24 hours of any security incident involving District data)

All District data must be encrypted and stored on US-based infrastructure. Large-scale exfiltration of real student or staff data is prohibited. Vendors must certify secure destruction of District data within 30 days.

---

7. Vendor Qualifications and Vetting

7.1 Vendor Inquiries

Pre-NDA clarification questions must be submitted to: **rfp@ffc8.org**

All inquiries will be vetted prior to release of supplemental information.

7.2 Minimum Vendor Qualifications

Vendors must provide:

- Experience conducting penetration testing in hybrid Active Directory and cloud identity environments
- Experience with public sector or regulated organizations
- Understanding of FERPA, COPPA, and applicable student data privacy laws
- Identification of assigned personnel
- Sample redacted penetration test report
- Example of documented multi-stage attack path narrative
- Proof of cybersecurity liability insurance with minimum coverage of $3,000,000
- Confirmation of background check compliance

Failure to provide required items may render the proposal non-responsive.

Vendors must disclose:

- Any financial interests or reseller relationships with security product manufacturers
- Any relationship or financial interest with Fountain-Fort Carson School District, its employees, students, school board members, or parents
- Whether subcontractors will be used

If subcontractors are used, the primary vendor must ensure all subcontractors:

- Meet the $3,000,000 cybersecurity liability insurance requirement
- Adhere to encrypted, US-based data storage requirements
- Complete required background checks

Payment

The District will complete payment via a Purchase Order; vendors must be able to accept Purchase Orders as the payment mechanism.

---

8. Proposal Format and Evaluation Criteria

Send the proposal to rfp@ffc8.org. Contact us if a secure method is required.

8.1 Required Proposal Format

A. Technical Approach and Validation Methodology
B. Internal Testing and Identity Approach
C. Remediation Approach and Prioritization
D. Operational Safeguards
E. Sample Report and Attack Path Example
F. Assigned Team Qualifications
G. Man-Day Allocation (≤5 total)
H. Pricing and Optional Retest Fees

8.2 Evaluation Criteria and Scoring

Scoring Scale

Proposals will be evaluated on a 0–5 scale using the following anchor points:

0 – Does not meet requirements; no credible evidence provided
3 – Adequately meets requirements; baseline capability demonstrated
5 – Exceptional; clearly differentiated, operationally mature approach supported by specific methodology and examples

Scores of 1, 2, and 4 may be assigned where proposals fall between anchor points. A score of 1 indicates material deficiency short of non-response; 2 indicates partial fulfillment; 4 indicates strong capability exceeding baseline but not fully exceptional.

Evaluators must score based on demonstrated evidence within the proposal. Claims lacking supporting methodology, examples, or detail will be treated as unsubstantiated. Volume of content does not compensate for lack of specificity.

Realistic scope prioritization within the defined five-person-day constraint will be weighted heavily.

Criterion	Weight
Validation Rigor & Technical Methodology	25%
Depth of Internal Testing & Identity Approach	25%
Remediation Approach and Prioritization Framework	20%
Clarity of Reporting & Business Impact Communication	15%
Operational Safeguards	10%
Assigned Team Experience	5%

AWARD NOTICE

The District is not obligated to award the lowest-cost proposal and may modify scope or decline to proceed. Proposals demonstrating realistic prioritization, validated attack path modeling where feasible, and structured remediation guidance will be evaluated most favorably.