



Dakota County Security Assessment RFP (2026) – Consolidated Vendor Q&A

1. Scope & Nature of Testing

a. Is testing of dakotacountymn.gov limited to external exposure validation, or does it include authenticated/unauthenticated web application and API testing?

Answer: Web app (www.co.dakota.mn.us): light-touch external review aligned to OWASP Testing Guide v4.0 only. No SAST/DAST, no deep authenticated web app/API or business-logic testing.

b. Will the assessment include external, internal, or both?

Answer: Both. External and Internal Network Penetration Tests are in scope.

c. Should the penetration test be black box, grey box, or white box?

Answer: The RFP does not mandate a model. Testing must start from hosts with zero pre-existing privileges; grey-box is more likely because the County will provide credentials/test accounts. Assume grey-box.

d. Should the assessment include lateral movement and persistence?

Answer: Include safe, controlled exploitation demonstrating real-world impact (initial compromise and limited pivoting). No red-team style persistence or destructive persistence testing.

e. Are critical/high value systems expected to receive deeper testing?

Answer: No special emphasis is required. Test all in-scope internal and external systems per the standard methodology.

f. Are wireless networks in scope?

Answer: No. Wireless testing is out of scope.

g. How many applications/URLs are in scope?

Answer: One public website: www.co.dakota.mn.us (cloud hosted), evaluate externally per OWASP guide.

h. Is the test being performed for compliance purposes?

Answer: Primarily a security posture validation and routine/audit assessment. No specific PCI/CJIS/HIPAA requirement is cited.

i. Are denial-of-service (DoS/DDoS) tests allowed?

Answer: DoS/DDoS testing is prohibited (destructive/availability-impacting testing on production is not allowed).

2. Asset Inventory & Environment Details

a. Will the County provide a final in-scope asset inventory?

Answer: Yes. The County will provide access, documentation, and an in-scope asset list (IP addresses, subnets, hostnames) after contract/NDA.

b. Number of external IPs and internal devices?

Answer: Proposal planning limits:

- External (public) live systems: < 100
- Internal (private) live systems/devices: < 600

c. Are cloud environments involved?

Answer: Only the public website (www.co.dakota.mn.us) is cloud hosted and in-scope for the light external review. Other cloud tenants (Azure/AWS/M365) are out of scope.

d. Will testing occur in production or non-production?

Answer: Testing will occur against production/live systems. No dedicated staging environment is provided by default.

e. From where is the application accessible?

Answer: The public website is Internet-accessible. Internal systems will be reachable from a County-approved testing host or via VPN as provided.

f. Typical OS and environment details?

Answer: Internal systems are primarily Windows Server and Linux. Systems are on-prem in two data centers (virtualization platforms may exist). More detailed environment data provided post-contract/NDA.

g. Can all internal live systems be reached from a single location?

Answer: Yes, internal systems are reachable from a single approved network location.

h. Are there special internal segments (CJIS, courts, etc.) requiring exclusions or clearances?

Answer: There may be excluded systems; the County will provide a definitive in-scope and excluded list. No special CJIS clearances are indicated in the RFP; if any segment requires special handling it will be identified post-award.

3. Access, Credentials & Testing Model

a. What access will be provided?

Answer: The County will provide necessary credentials, test accounts, and VPN access if required/approved. Vendors should propose both credentialed and unauthenticated approaches as applicable.

b. How many user roles are in scope?

Answer: User-level accounts only; no broad user population testing. Test accounts will be non-privileged unless otherwise provided.

c. Session management, WAF, multi-tenancy, CMS?

Answer: Not applicable for deep app testing. Provide OWASP external checks only for the public website. Details about WAF or CMS (if present) will be provided post-award if relevant to the external review.

d. Will vendors need CJIS training or fingerprint-based clearances?

Answer: None specified. If special clearances are required for any particular systems, the County will notify vendors post-award.

e. Background checks?

Answer: Not generally required by the RFP.

f. Any tools whitelist?

Answer: No formal whitelist is published. Vendors must list intended tools; any restrictions will be provided post-award.

4. Web Application / API Testing Details

All detailed web application/API testing items are NOT APPLICABLE except for a light-touch OWASP external review of www.co.dakota.mn.us. No SPA/API deep testing, no SAST/DAST, no authenticated business-logic testing. The “Note” referencing web application testing can be ignored for deep application testing.

If vendor asks about size/structure of website: the County will provide details post-award; expect a mix of static and dynamic pages and a standard public CMS/portal footprint, only external OWASP checks required.

5. Timeline, Testing Windows & Restrictions

a. Expected testing windows, blackout dates, after hours restrictions?

Answer: Schedule to be coordinated after contract signature. Testing during business hours is acceptable; after-hours/weekends are likely allowable. The vendor must have a suspension/throttling process to stop/testing if operational impact occurs. Specific blackout dates (if any) will be provided after award.

b. Who are the escalation contacts during testing?

Answer: The County will provide escalation contacts to the awarded vendor.

c. Expected duration of testing, reporting, and retesting?

Answer: Contract period: July 13, 2026 – September 21, 2026. All testing, reporting, and any agreed retesting must be completed within the contract term unless otherwise negotiated.

d. Expected schedule for active testing phase?

Answer: The exact start date, duration, and key milestones for active testing will be coordinated with the awarded vendor. Vendors should propose a reasonable testing duration and timeline in their proposals.

e. Onsite vs remote preference?

Answer: Onshore resources are required but onsite presence is not mandatory. The engagement can run remotely; on-site visits are optional, and vendor may include travel cost assumptions. County has no strict preference; historically both remote and hybrid have been used.

f. Status reporting cadence during testing?

Answer: Negotiable; suggest milestone-based or weekly status updates. County will expect reasonable responsiveness to vendor communications during active testing.

6. Reporting Requirements

a. What severity/risk rating methodology should be used?

Answer: Vendors may use their standard methodology (CVSS or equivalent). Provide clear mapping from vendor ratings to CVSS or an explanation. Tailor executive summary for C-suite.

b. Requirements for delivery, encryption, retention, and distribution of evidence?

Answer: Reports must meet WCAG 2.1 Level AA accessibility for digital content. Delivery method negotiable but must be encrypted. Supporting evidence archives (tool outputs, raw data) must be provided; vendors must specify retention and secure delivery.

c. Must full scan outputs be submitted?

Answer: Yes. An archive of all tool output (supporting data archive) is required.

d. Environment Parity Validation Report requirement?

Answer: Not applicable, this requirement relates to application parity and is not applicable to this network-focused assessment.

e. Report format and level of detail expectations?

Answer: Provide a balance of executive summary, prioritized findings with affected assets, remediation guidance, and technical details for triage. The County appreciates exportable outputs (CSV/Excel) or a downloadable archive rather than only a vendor-locked dashboard.

f. Accessibility Conformance Report / VPAT?

Answer: Deliverables must meet WCAG 2.1 AA. A self-attestation is acceptable unless the County requests a formal VPAT post-award.

7. Remediation & Retesting

a. Is remediation retesting included?

Answer: RFP references a remediation retest window (example: 30 days). Historically, remediation validation is minimal, and vendor involvement is limited to calls and limited

retesting. Vendors should propose whether retesting is included in base scope or offered as an option; include retest pricing and timing assumptions.

b. Is remediation validation required for all findings?

Answer: Not specified. Vendors should propose a standard remediation validation approach and whether retesting is included or optional.

8. Social/Physical/Wireless/Other Out-of-Scope Items (explicit)

a. Wireless network testing?

Answer: Out of scope.

b. Social engineering (phishing/vishing/smishing)?

Answer: Out of scope.

c. Physical security testing?

Answer: Out of scope.

d. Cloud tenant assessments (beyond public website) and M365?

Answer: Out of scope unless explicitly added later.

9. Operational / Logistics / Security

a. Will the County host vendor-supplied testing appliance?

Answer: Remote VPN access is expected; on-prem appliance can be discussed post-award if needed.

b. Who are the points of contact and expected availability?

Answer: The County will provide named points of contact and escalation contacts after award. Expect at least primary technical and project manager contacts; availability details to be provided post-selection.

c. IT/Security staffing and monitoring tools?

Answer: IT staff ~65, Security staff ~2. The County uses Tenable.io for vulnerability management. Details on monitoring/SOC tools are operationally sensitive and will be shared post-NDA.

d. Detection & response validation?

Answer: Not required as a primary objective. If vendors propose detection-testing or D&R validation, include it as optional with clear scope and non-disruptive methods.

e. Geographic/site differences or prioritization?

Answer: None. No special regional considerations.

10. Pricing, Procurement & Administrative

a. Is there an incumbent vendor?

Answer: Past assessments exist; the most recent large assessment (2024). No incumbent is guaranteed to participate; the County intends to contract with a single firm.

b. Budget / Not-to-Exceed (NTE) amount?

Answer: No set budget is published. Historical range for similar engagements: \$20,000 to \$100,000 depending on scope. This year's assessment is smaller; vendors should propose cost structures accordingly.

c. How should pricing be submitted?

Answer: Break down pricing by major sections (external, internal, reporting, optional retest, travel/reimbursables). Include hourly rates per role, estimated hours per role, and a maximum not-to-exceed total. If internal and external rates are identical, one line item is acceptable. Travel may be included or proposed as reimbursable, specify approach.

d. Are electronic signatures acceptable?

Answer: Yes, electronic signatures are acceptable for proposal forms unless otherwise specified in procurement instructions.

e. Trade secret / confidential submission format?

Answer: Provide one unredacted copy and one redacted copy per RFP instructions to request trade-secret treatment. Follow instructions in the confidentiality section of the RFP.

f. Local references requirement?

Answer: "Local" references are requested but not mandatory; similar government cybersecurity assessment experience outside the immediate area is acceptable. Provide relevant public-sector references; commercial references are acceptable.

g. Will the County award to one or multiple vendors?

Answer: A single vendor will be selected.

h. Proposal evaluation and best value?

Answer: The County considers technical approach, experience, and cost; they are not restricted to the lowest bidder and may select best value. Exact weighting is not specified.

i. Minority-owned business goals?

Answer: No specific minority procurement goals are in effect for this RFP.

j. Will vendor interviews/demos be required?

Answer: County may conduct interviews, presentations, or demonstrations as part of evaluation; include availability for interviews in your proposal.

11. Deliverable Expectations & Formats

a. Expected deliverables?

Answer: Executive summary (C-suite), full technical report, prioritized findings with affected assets, remediation guidance, supporting data archive (all tool output), and digital content

meeting WCAG 2.1 AA. Provide exportable formats (CSV/Excel) for findings and an evidence bundle. If vendor uses a dashboard, ensure data can be exported for County retention.

b. Level of detail for reports?

Answer: Executive summary for non-technical executives; technical sections sufficient for remediation teams including affected hosts, evidence, and remediation steps. Avoid vendor-locked raw dumps (e.g., raw Nessus exports without context).

c. Sample reports?

Answer: Vendors may include sample reports with proposals.

12. Submission Guidance for Vendors

- Propose a clear scope based on the RFP and this Q&A. Distinguish base scope (internal + external network tests + OWASP light external website review) from optional services (deep web app testing, phishing, DoS testing, extensive retesting, detection validation).
- Provide pricing broken out by major sections, hourly rates per role, estimated hours, and NTE. Clearly mark optional items and retesting costs.
- Include sample reports, exportable findings format, and confirmation you will deliver supporting tool output in an encrypted archive.
- Include staffing details (onshore resources), relevant references (government/corporate), and availability for coordination/interviews.
- Indicate whether retesting is included or optional and the proposed retest window (suggest 30 days or specify alternate).
- List required County support (e.g., credentials, VPN access, SIEM/EDR log access) needed to perform proposed detection validation or authenticated testing.
- Insurance: provide cyber liability insurance evidence per RFP/contract instructions; County may require proof prior to contract execution or testing.
- Follow trade-secret submission instructions in the RFP if requesting confidentiality.

13. Additional Clarifications

- Log access: SIEM/EDR log access is not guaranteed; will be provided under NDA if detection validation is agreed.
- Stealth and detection testing: include as optional with explicit procedures and escalation/stop conditions.

Note: *This document contains the consolidated questions and answers received during the initial publication of the Dakota County Security Assessment RFP. Because this solicitation is being republished, the County is including the same Q&A with the second publication to provide all prospective respondents with equal access to the clarifications issued during the original solicitation period.*