



STATE OF NORTH CAROLINA  
STATE BUREAU OF INVESTIGATION

JOSH STEIN  
GOVERNOR

R.E. "CHIP" HAWLEY  
DIRECTOR

**SOLICITATION ADDENDUM**

Issuing Agency:	State Bureau of Investigation
Solicitation Number:	49-250811-BH
Solicitation Description:	Website Development, Hosting and Content Management Services
Solicitation Opening Date and Time:	May 19, 2026 / 2:00 PM EST
Addendum Number:	1
Addendum Date:	May 12, 2026
Procurement Specialist:	Boyce Haywood

**THIS ADDENDUM DOES NOT NEED TO BE RETURNED.**

- The following are questions received about the Solicitation and the State's response to those questions:

Question #	Solicitation Section	Vendor Question	State's Response
1.	General	Is there a current vendor providing any portion of the services described in this RFP (e.g., hosting, CMS, portal authentication, content management)? If so, please describe the scope of their current engagement, the contract end date, and whether any transition services are anticipated.	<b>Capitol Broadcasting currently provides the landing page only, with the contract to be renewed through December 2026. No transition services are anticipated; the new Solution will replace the landing page upon go-live.</b>
2.	2.1 Purpose of RFP	Please confirm that a Drupal-based solution is fully acceptable and will be evaluated equally with WordPress, provided it meets all mandatory security, hosting, accessibility, and portal requirements.	<b>Confirmed. Drupal-based and WordPress-based solutions will be evaluated equally provided all mandatory security, hosting, accessibility, and portal requirements are met.</b>
3.	2.3 Summary of Problem Statement	Is there an expected phased release roadmap or minimum viable product scope for the initial production launch, or should vendors propose the phasing approach?	<b>Vendors shall propose the phasing approach. The implementation timeline must accommodate the RISE Back to School Safety Summit; vendors may propose phased releases by audience or feature set.</b>

Question #	Solicitation Section	Vendor Question	State's Response
4.	2.3 Summary of Problem Statement	Section 2.3 describes '4 separate access portals' but lists five items (including 'Vision for the solution'). Please confirm that the 'Vision for the solution' is narrative and the total remains four portals.	<b>Confirmed — there are four (4) portals total. The 'Vision for the Solution' is narrative.</b>
5.	2.3 Summary of Problem Statement	Please clarify whether the four portals should be implemented as four distinct sites, four sections within one site, or a single application with audience-based routing and permissions.	<b>The four portals shall be implemented as four sections under a single 'Training Portals' tab on a single multi-site CMS configuration with audience-specific menus and content. See also Q115, Q134, Q246.</b>
6.	2.3 Summary of Problem Statement	Section 2.3 states the Student and General Public Portals 'will be unsecure,' while Section 3.3.3 and REQ-010b describe email-based authentication for all four portals. Please reconcile these and confirm whether the Student and General Public Portals require authentication.	<b>Reconciled: the Student Portal and General Public Portal shall be unsecured (no authentication, no PII collection). Email-based authentication with MFA applies only to the Law Enforcement and Admin/Teacher portals.</b>
7.	2.3 Summary of Problem Statement	Section 2.3 states the Law Enforcement and Admin/Teacher portals will use two-factor authentication, but Section 3.3.3 describes MFA only for external contributors. Please clarify whether MFA is required for all registrants of those portals or only for administrative roles.	<b>Authentication model by portal: (1) Student Portal — unauthenticated public access, no PII collection, no account creation; (2) General Public Portal — unauthenticated public access, no PII collection; (3) Admin/Teacher/Support Staff Portal — email-based registration validated against approved LEA / charter school / education staff domains, MFA required for all users, manual approval by CFSS; (4) Law Enforcement Portal — email-based registration validated against approved law enforcement agency domains (.gov / .us), MFA required for all users, manual approval by CFSS. The earlier reference to MFA only for 'external contributors' is superseded by this clarification.</b>
8.	2.3 Summary of Problem Statement	For Law Enforcement and Admin/Teacher portal users authenticated by email domain, does the State require persistent user accounts tied to individual email addresses, or is stateless domain-based authentication (no per-user account stored) acceptable? This significantly affects sizing and cost.	<b>Individual user accounts tied to a state, local government, agency, or school email address are required. Stateless domain-based authentication is not acceptable.</b>

Question #	Solicitation Section	Vendor Question	State's Response
9.	2.3 Summary of Problem Statement	The addressable populations (~1.7M students and ~2M general public) are very large. What are the State's expected adoption rates and concurrent-user targets by Year 1, Year 3, and Year 5 for infrastructure sizing?	<b>The State does not have historical analytics for the existing single landing page (currently provided by Capitol Broadcasting; no meaningful traffic data available). Adoption rate targets and concurrent user counts for Years 1, 3, and 5 are not available. Addressable populations stated in Section 2.3 are upper bounds. Vendors shall propose tiered pricing and capacity assumptions; recurring pricing should assume FedRAMP Moderate hosting with standard business-hours support, with 24x7 / premium support priced as an optional service. Anticipated peak conditions occur prior to and following large events such as the RISE Back to School Safety Summit, and prior to the start of the school year.</b>
10.	2.3 Summary of Problem Statement	What is the expected age range of Student Portal registrants (e.g., grades 6-12, or all K-12)? This determines COPPA applicability and authentication approach for users under 13.	<b>Likely age range for Student Portal users is grades 6–12. Because no PII will be collected and no accounts created (the Student Portal is unsecured public access for video and informational content only), COPPA parental consent workflows are not required. See also Q91, Q116, Q132, Q152, Q159, Q197.</b>
11.	2.4 Contract Term	Please confirm that pricing for Years 4 and 5 (renewal options) should be firm-fixed at offer submission and will be exercised at the State's sole discretion.	<b>Yes, prices are to be firm-fixed price.</b>
12.	2.6 Contract Type	Given that hosting and recurring services scale with user population, will the State clarify what constitutes the 'definite quantity' under the Definite Quantity Contract for pricing and commitment purposes?	<b>The definite quantity is defined as what the required associated cost are as outlined in Attachment D: Cost Form. The definite quantity is if one-time implementation cost or recurring annual cost.</b>

Question #	Solicitation Section	Vendor Question	State's Response
13.	3.2.2 Security Specifications	What retention period is required for audit logs, content change logs, administrative action logs, and authentication logs?	<b>Audit logs, authentication logs, content change logs, and administrative action logs shall be retained for a minimum of 365 days online and 3 years total (online + archived). Logs must be tamper-evident and exportable to the State on request. Media library files shall have version control and activity tracking equivalent to page/post edits.</b>
14.	3.2.2 Security Specifications	Are there State-required change management workflows or approvals that should be built into the deployment and release process?	<b>All production changes require a formal change management workflow with versioning, rollback capability, and audit logging. NC SBI IT must approve all production changes affecting security configuration, integration endpoints, or authentication. Routine content updates by CFSS authorized users do not require NC SBI IT approval but must be logged.</b>
15.	3.2.2 Security Specifications	If the underlying IaaS/PaaS provider holds FedRAMP Moderate authorization and the vendor's SaaS layer holds SOC 2 Type 2, will the combination be accepted to satisfy Section 3.2.2(b)? What documentation is required to demonstrate coverage of the SaaS layer?	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>

Question #	Solicitation Section	Vendor Question	State's Response
16.	3.2.2 Security Specifications	Section 3.2.2 characterizes the data as 'Low Risk (Public)' but requires NIST 800-53 Moderate controls. Please confirm the solution is not expected to process CJIS data, PII of minors beyond minimal registration data, or other moderate/high-risk data classifications.	<b>Data classification is Low Risk (Public). NIST SP 800-53 Moderate baseline controls are firm and required regardless of classification, due to the Solution's exposure to law enforcement users, school personnel, and minors. The Solution shall not process Criminal Justice Information (CJI) or PII of minors beyond minimal account registration data for authenticated portals (Law Enforcement and Admin/Teacher portals only).</b>
17.	3.2.2 Security Specifications	Will the State provide the current VRAR template and confirm whether a full control-by-control narrative is required at offer submission, or a summary attestation with detail deferred to contract award?	<b>The current VRAR template will be made available with this Addendum or upon Vendor request to the Procurement Specialist. A summary attestation at offer submission with detailed control-by-control narrative deferred to award is acceptable, provided the summary is sufficient to evaluate inheritance and gaps.</b>
18.	3.3.2 Solution Architecture	Does the State have existing enterprise licensing or hosting relationships (e.g., Pantheon, Acquia, WP Engine, Azure Government, AWS GovCloud) that vendors should leverage or align with under Section 3.1.5?	<b>The State has Microsoft enterprise relationships (M365, Entra ID) but is not designating an enterprise CMS hosting platform vendors must use. Pantheon, Acquia, WP Engine, Azure Commercial, AWS commercial, and similar platforms are acceptable provided FedRAMP Moderate hosting and U.S. data residency requirements are met.</b>
19.	3.3.3 Identity and Access Management	Will the State provide Entra ID application registration, metadata, test accounts, required claims/attribute mapping, and a coordination point for the IdP integration? (Also addresses REQ-006 and REQ-010e.)	<b>Entra ID authentication is for the 2-3 CFSS administrative users only. End users of the Law Enforcement and Admin/Teacher portals authenticate via the email-based registration model with MFA described above, not via Entra ID. NC SBI will provide Entra ID application registration, metadata, test accounts, attribute mapping, and a coordination point for the limited Entra ID integration. A non-production / sandbox Entra ID environment will be made available prior to UAT.</b>

Question #	Solicitation Section	Vendor Question	State's Response
20.	3.3.3 Identity and Access Management	Please confirm that the '2-3 users' (NC SBI AD) and 'up to 6 users' (external contributors) represent total content-management user counts across the contract term, separate from portal registrant populations.	<b>Confirmed — the '2–3 users (NC SBI AD)' and 'up to 6 external contributors' represent total content-management user counts across the contract term, separate from portal registrant populations.</b>
21.	3.3.3 Identity and Access Management	For the up to six external contributors, should those users authenticate through local platform accounts, a separate identity provider, or email-based passwordless/MFA login?	<b>External contributors shall authenticate with email-based registration plus MFA, with manual approval by CFSS.</b>
22.	3.3.3 Identity and Access Management	For email-domain validation on the Law Enforcement Portal (agency .gov/.us domains) and the Admin/Teacher Portal (LEA and charter school domains), will the State provide the authoritative lists and handle updates, or is the vendor expected to curate and maintain them?	<b>CFSS will adjudicate all registration requests. The Vendor shall provide a master list / dashboard of approved users accessible to CFSS administrators, with workflow for approval, denial, suspension, and removal. CFSS does not maintain a pre-existing authoritative domain list; the approval-on-request model replaces blanket domain whitelisting. The Vendor is not required to research or maintain external domain lists.</b>
23.	3.3.3 Identity and Access Management	Should portal users be self-approved based solely on email domain, require manual CFSS approval, require invitation-only registration, or follow different workflows by portal audience?	<b>All registration requests will be manually approved by CFSS. Self-approval based on email domain alone is not acceptable for the Law Enforcement and Admin/Teacher portals.</b>
24.	3.3.3 Identity and Access Management	Please define the required platform roles and permissions beyond Administrator, Editor, Author, and Viewer — especially for portal managers, trainers, reviewers, approvers, and external contributors.	<b>The Vendor shall implement role-based access control (RBAC) with at minimum the following roles: Administrator, Editor, Author, Viewer, Portal Manager, Approver. Vendor may propose additional granular roles. The State prefers least-privilege; full Administrator privileges shall be limited to the smallest practical set of accounts</b>

Question #	Solicitation Section	Vendor Question	State's Response
25.	3.3.4 Integration Approach	For Power BI dashboards: (a) will embeds be public, secure, or tenant-authenticated; (b) will dashboards live in the State's existing Power BI tenant or require a vendor-provided workspace; and (c) who bears Power BI Pro/Premium licensing cost?	<b>The following are currently licensed and in use by CFSS / NC SBI and will be made available for integration: Microsoft 365 (including Teams), YouTube (public), Whova, Eventbrite, Google Workspace (where used by CFSS), Microsoft Forms / Microsoft cloud surveys. Power BI licensing model for embedding shall be confirmed during discovery; if Power BI Embedded capacity licensing is required for the proposed embedding model, the Vendor shall include this in the cost proposal as a separately identified line item. Domain / DNS, SSL certificates, and email/transactional messaging services associated with the new platform shall be included in Vendor pricing.</b>
26.	3.3.4 Integration Approach	Are Whova and Eventbrite examples only, or are there required event registration platforms that the platform must support at launch?	<b>Whova and Eventbrite are required event registration platforms that the platform must support at launch via embed or integration. Native registration / waitlist / capacity / reminders functionality within the platform is not required and may be handled by the third-party tools.</b>
27.	3.3.4 Integration Approach	Should surveys be implemented natively in the platform, embedded from third-party services, or both? If specific third-party platforms are required, please identify them.	<b>Surveys may be implemented natively in the platform or embedded from third-party services. Microsoft Forms (Microsoft cloud) is the State's primary tool. Either integrated forms (e.g., Gravity Forms) keeping submissions on-platform, or embedded Microsoft Forms, is acceptable. Vendor shall propose both options and identify trade-offs.</b>
28.	3.3.4 Integration Approach	For Google Workspace integrations (Sheets, Docs, Calendar), will CFSS provide service-account credentials and cover Workspace licensing, or is the vendor expected to procure and manage these?	<b>Where Google Workspace integration is needed for embedded Sheets, Docs, or Calendar content, CFSS will provide service account credentials and bear Workspace licensing for content owned by CFSS. The Vendor is not expected to procure Workspace licenses but shall handle integration configuration.</b>

Question #	Solicitation Section	Vendor Question	State's Response
29.	3.3.5 Disaster Recovery	Do the RPO ≤ 24 hours and RTO ≤ 4 hours apply to the full production environment including all portals and embedded content, or only to core CMS content? Also, must DR failover be automatic, or is a documented manual runbook acceptable?	<b>Recovery Point Objective (RPO) ≤ 24 hours and Recovery Time Objective (RTO) ≤ 4 hours apply to the full production environment, including all four portals and the CMS-managed embedded content references. Embedded third-party content (Power BI, YouTube, Google Workspace) availability is governed by those providers. Documented manual runbook with tested annual failover is acceptable; fully automatic failover is not required. Off-site, immutable backups isolated from the primary hosting environment are required to defend against ransomware / destructive attack scenarios.</b>
30.	3.3.6 Data Migration	Although no data migration is required, should the vendor include content entry, starter content loading, menu setup, or migration from the current NC SBI school safety page? If so, please indicate approximate volume.	<b>There is minimal content migration. The current <a href="https://ncsbi.gov/Services/School-Safety">ncsbi.gov/Services/School-Safety</a> landing page (Capitol Broadcasting) is the only existing source. CFSS's training calendar from the prior <a href="https://cfssnc.gov">cfssnc.gov</a> website shall be migrated. No bulk document, video, or dashboard migration is required. Vendors are not responsible for accessibility remediation of legacy content not migrated.</b>
31.	3.3.7 Application Management	Are there specific State monitoring tools, dashboards, alerting integrations, or notification channels that the hosting environment must integrate with?	<b>The Vendor shall provide hosting environment monitoring with email alerting to a CFSS distribution list and NC SBI IT distribution list for Severity 1 and Severity 2 incidents. No State-mandated monitoring tool integration is required. The Vendor shall provide exportable monthly availability and performance reports.</b>
32.	3.3.7 Application Management	How frequently should access reviews occur, and should the platform provide exportable access review reports for CFSS administrators?	<b>Access reviews shall occur at minimum quarterly for the Law Enforcement and Admin/Teacher portals, and annually for administrative roles. The platform shall provide exportable access review reports.</b>

Question #	Solicitation Section	Vendor Question	State's Response
33.	3.3.8 Accessibility	Is the vendor responsible for accessibility compliance (WCAG conformance) of content supplied by the State, or only for the platform, vendor-built templates, and content the vendor creates?	<b>WCAG 2.1 Level AA conformance is required, in addition to Section 508. The Vendor is responsible for accessibility of: the platform itself, vendor-built templates, vendor-developed components, and content the Vendor creates or initially populates. CFSS is responsible for accessibility of content CFSS uploads after launch (closed captions on CFSS-produced videos, accessible PDFs, alt text on uploaded images), with vendor-provided tooling and guidance.</b>
34.	3.4.1 Platform Requirements	Under REQ-001, are there any required or prohibited Drupal distributions, hosting platforms, contributed modules, or commercial Drupal services that vendors should account for?	<b>Both Drupal and WordPress are acceptable and will be evaluated equally, provided all mandatory security, hosting, accessibility, and portal requirements are met. There is no internal preference. Managed WordPress / Drupal platforms (e.g., Pantheon, Acquia, WP Engine) hosted by a third-party platform provider are acceptable if FedRAMP Moderate, U.S. data residency, and U.S. personnel requirements are met, and the prime Vendor remains responsible for implementation, support, and compliance. The State has not standardized on NC Digital Commons for this procurement; vendors may propose, but it is not required.</b>

Question #	Solicitation Section	Vendor Question	State's Response
35.	3.4.1 Platform Requirements	REQ-002 requires US-based hosting including DR. Is a FedRAMP-authorized commercial cloud region (e.g., AWS us-east, Azure Commercial) sufficient, or does the State require GovCloud / Azure Government or in-state (NC) data centers?	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>
36.	3.4.1 Platform Requirements	Will the State accept the vendor's standard SLA credit schedule as the 'documented remedies for non-compliance' under the 99.9% uptime SLA, or are specific liquidated-damages amounts required? If the latter, please provide the schedule.	<b>99.9% uptime SLA is required, measured monthly excluding scheduled maintenance windows. The Vendor's standard service credit schedule is acceptable as the documented remedy for non-compliance, provided credits are meaningful (minimum 5% of monthly recurring fees per 0.1% below SLA, escalating). Specific liquidated damages are not required. Auto-scaling shall absorb traffic surges typical of post-event and pre-school-year periods without service degradation; specific surge multipliers are not mandated, but the Vendor's proposed scaling capacity will be evaluated.</b>
37.	3.4.2 Authentication and Access Control	Should the maximum 30-minute inactivity timeout apply to all authenticated portal users, or only to administrators, editors, authors, and external contributors?	<b>The 30-minute inactivity timeout applies to all authenticated portal users (Law Enforcement and Admin/Teacher portals), not only to administrative roles.</b>

Question #	Solicitation Section	Vendor Question	State's Response
38.	3.4.2 Authentication and Access Control	Beyond FERPA and COPPA, does REQ-010e's 'applicable student data privacy requirements' include specific North Carolina statutes (e.g., Student Online Personal Information Protection Act) or LEA-level data-sharing agreements?	<b>Beyond FERPA, COPPA, Section 508, and WCAG 2.1 AA, the following also apply: applicable provisions of the North Carolina Student Online Personal Information Protection Act and any LEA-level data-sharing agreements that may apply to specific content. Detailed legal review will occur during contracting; vendors shall represent in good faith that they can support these requirements.</b>
39.	3.4.3 Content Management Requirements	For REQ-012 document uploads, what maximum file sizes, file types, storage volumes, virus scanning requirements, and retention/versioning requirements should the platform support?	<b>REQ-012 document upload parameters: maximum individual file size 100 MB; supported types include PDF, DOCX, XLSX, PPTX, common image formats, and approved video formats; total storage shall scale with content; virus scanning of all uploads is required; minimum 10 prior versions retained per file; file retention follows the State's records retention schedule.</b>
40.	3.4.3 Content Management Requirements	Should content scheduling and revision rollback apply to all content types — including training content, documents, event listings, portal pages, and embedded resources?	<b>Yes — content scheduling and revision rollback shall apply to all content types including training content, documents, event listings, portal pages, and embedded resources</b>
41.	3.4.4 Performance and Scalability	For REQ-019 performance sizing, please provide expected launch traffic, peak traffic during high-profile events, and target concurrent authenticated users.	<b>The State does not have historical analytics for the existing single landing page (currently provided by Capitol Broadcasting; no meaningful traffic data available). Adoption rate targets and concurrent user counts for Years 1, 3, and 5 are not available. Addressable populations stated in Section 2.3 are upper bounds. Vendors shall propose tiered pricing and capacity assumptions; recurring pricing should assume FedRAMP Moderate hosting with standard business-hours support, with 24x7 / premium support priced as an optional service. Anticipated peak conditions occur prior to and following large events such as the RISE Back to School Safety Summit, and prior to the start of the school year.</b>

Question #	Solicitation Section	Vendor Question	State's Response
42.	3.4.4 Performance and Scalability	How will the 3-second average page-load requirement be measured — by page type, geography, network conditions, authenticated vs. anonymous, and inclusion or exclusion of third-party embeds (Power BI, Google Workspace, video)?	<b>The 3-second average page-load requirement shall be measured: (a) for representative authenticated and unauthenticated public-facing pages, (b) using synthetic monitoring from at least one U.S. East and one U.S. Central monitoring location, (c) under typical broadband network conditions, (d) for first-byte and document-complete metrics excluding third-party embedded content load time (Power BI, Google Workspace, video). Vendors shall propose the specific page templates to be measured.</b>
43.	3.4.5 Training Requirements	How will the 3-second average page-load requirement be measured — by page type, geography, network conditions, authenticated vs. anonymous, and inclusion or exclusion of third-party embeds (Power BI, Google Workspace, video)?	<b>The 3-second average page-load requirement shall be measured: (a) for representative authenticated and unauthenticated public-facing pages, (b) using synthetic monitoring from at least one U.S. East and one U.S. Central monitoring location, (c) under typical broadband network conditions, (d) for first-byte and document-complete metrics excluding third-party embedded content load time (Power BI, Google Workspace, video). Vendors shall propose the specific page templates to be measured.</b>
44.	3.5.1 Website Design and UX	Does CFSS have existing brand guidelines, logos, sitemap, design system, or content inventory that must be followed, or is the vendor expected to propose a design concept and information architecture?	<b>Yes — CFSS has existing logos and a blue/white visual theme that must be applied. Two current logos will be provided. Vendors shall use these existing identity elements as the foundation; full brand discovery / new identity development is not in scope. Vendors should plan for content strategy, information architecture, page templates, navigation, plain-language editorial review, and accessibility tagging as part of base scope. Some content creation support is expected — see content authoring response.</b>

Question #	Solicitation Section	Vendor Question	State's Response
45.	3.5.1 Website Design and UX	How many distinct page templates, content types, and initial content pages should the vendor plan to design and build at launch? A rough target assists accurate pricing.	<b>Initial design and build target: estimated 6-10 distinct page templates, 8-12 content types, and 30-60 initial content pages across the public site and four portals. Vendors should plan accordingly; final scope confirmed during discovery. Two design concepts and 1-2 rounds of revisions are expected; clickable prototypes are preferred.</b>
46.	3.5.1 Website Design and UX	Should search cover only platform-managed content, or should it also index uploaded documents, training materials, embedded Google Workspace content, Power BI dashboards, and video metadata?	<b>Search shall cover platform-managed content, uploaded documents, and training materials. Embedded Google Workspace content, Power BI dashboards, and video metadata are out of scope for full-text indexing.</b>
47.	3.5.2 Content Workflow and Collaboration	Please define the desired editorial workflow stages, reviewer roles, approval authority, and whether separate workflows are needed for public pages versus restricted training portal content.	<b>Separate editorial workflow paths are required by program area, portal, and content type. Vendor shall propose a workflow capable of supporting at minimum: public content workflow, restricted training portal workflow, and law enforcement portal workflow, each with editor → reviewer → approver stages. CFSS will define final reviewer / approver assignments during discovery.</b>
48.	3.5.3 Analytics and Reporting	Is Google Analytics acceptable for this State law enforcement division site, or is a privacy-focused or State-approved analytics platform required?	<b>Google Analytics is acceptable for this site. Vendor shall confirm cookie banner and privacy notice meet North Carolina and FERPA / COPPA expectations given the audience includes minors (even though no PII is collected). LMS-specific user progress data combined with Google Analytics satisfies the user activity tracking requirement.</b>

Question #	Solicitation Section	Vendor Question	State's Response
49.	3.5.3 Analytics and Reporting	Should the platform track training completion, course progress, quiz results, attendance for live sessions, and certificates — or only page/content engagement metrics?	<b>The State requires pre-test and post-test capability for Law Enforcement and Admin/Teacher portal training. Vendors shall propose an LMS solution capable of pre/post assessments, individual completion tracking, basic quiz scoring, and exportable completion records for those two portals. Full SCORM/xAPI conformance, continuing education unit (CEU) tracking, and formal certificates are not required at launch but should be supported on the platform roadmap. The Student Portal hosts video content for a video competition only, with no individual progress tracking. The General Public Portal requires no LMS functionality.</b>
50.	3.5.4 Support Services	The Cost Form lists 'Premium Support (24/7)' as optional, suggesting base is business hours. Please confirm the required base service level (e.g., 8x5 business hours vs. extended vs. 24x7).	<b>Confirmed — base support level is business hours (Monday – Friday, 8:00 AM – 5:00 PM Eastern, excluding State holidays). Premium 24x7 support is optional. Severity 1 incidents shall have 24x7 response per Section 7.15.</b>
51.	3.5.4 Support Services	What maintenance windows, patch deployment timelines, core/contributed module update frequency, and emergency security patch expectations should vendors assume?	<b>Routine patching shall occur within the standard maintenance window (vendor-proposed off-hours). Critical / High security patches per the cadence in the security response. Module / core updates monthly at minimum; Vendor shall maintain currency within one major version of supported releases.</b>
52.	3.5.4 Support Services	Will the State require ongoing site enhancement support beyond maintenance? If yes, please provide an estimated monthly or annual budget of hours so vendors can price consistently.	<b>Annual enhancement / change request budget shall be priced as a not-to-exceed pool of hours (vendor proposes; the State suggests planning for approximately 200 – 400 hours per year). The State prefers a fixed annual fee for proactive patching, updates, and routine enhancement; T&amp;M billing is acceptable for discrete change requests beyond the pool.</b>

Question #	Solicitation Section	Vendor Question	State's Response
53.	3.5.4 Support Services	For proactive patching, updates, and enhancement work, does the State prefer a fixed annual fee or T&M billing?	<b>Annual enhancement / change request budget shall be priced as a not-to-exceed pool of hours (vendor proposes; the State suggests planning for approximately 200 – 400 hours per year). The State prefers a fixed annual fee for proactive patching, updates, and routine enhancement; T&amp;M billing is acceptable for discrete change requests beyond the pool.</b>
54.	3.5.5 Future Capabilities	Please provide examples of anticipated future database-driven features so the platform architecture can be designed for likely expansion without overbuilding the initial scope.	<b>Future database-driven feature examples include: searchable directory of school resource officers / safety contacts, interactive grant or program lookup, threat assessment resource library with role-based filtering, structured incident reporting for non-emergency school safety concerns. Architect for extensibility; do not pre-build.</b>
55.	3.5.6 Training Portal Specifications	Should each portal have distinct branding/navigation and landing pages, or should all portals share a common theme with audience-specific menus and content listings?	<b>Common platform theme with audience-specific menus and content listings. Distinct branding per portal is not required</b>
56.	3.5.6 Training Portal Specifications	For pre-recorded video courses, does CFSS require a full LMS with SCORM/xAPI, completion tracking, quizzes, and certificates — or is video streaming with basic view-tracking sufficient?	<b>The State requires pre-test and post-test capability for Law Enforcement and Admin/Teacher portal training. Vendors shall propose an LMS solution capable of pre/post assessments, individual completion tracking, basic quiz scoring, and exportable completion records for those two portals. Full SCORM/xAPI conformance, continuing education unit (CEU) tracking, and formal certificates are not required at launch but should be supported on the platform roadmap. The Student Portal hosts video content for a video competition only, with no individual progress tracking. The General Public Portal requires no LMS functionality</b>

Question #	Solicitation Section	Vendor Question	State's Response
57.	3.5.6 Training Portal Specifications	For live/scheduled virtual training sessions, will CFSS use an existing State-licensed platform (Zoom/Teams/WebEx) with the portal handling registration only, or is the vendor expected to provide the conferencing platform?	<b>Live and scheduled virtual training sessions will be hosted by CFSS using Microsoft Teams (externally accessible). The platform shall integrate registration only — calendar publishing, registration capture, reminders, and basic attendance reporting. The Vendor is not required to provide a web conferencing platform.</b>
58.	3.5.6 Training Portal Specifications	Should the platform manage registration capacity, waitlists, reminders, attendance, and calendar invites for live sessions, or may these functions be handled by embedded third-party tools?	<b>Whoova and Eventbrite are required event registration platforms that the platform must support at launch via embed or integration. Native registration / waitlist / capacity / reminders functionality within the platform is not required and may be handled by the third-party tools.</b>
59.	3.5.6 Training Portal Specifications	What is the estimated training content volume at go-live (hours of video, number of documents) and the expected annual growth? This is require CDND for storage and CDN sizing.	<b>Estimated training content volume at go-live is modest — approximately 10–25 videos and 25–50 documents, with annual growth of similar magnitude. Vendors shall size CDN and storage to a minimum of 500 GB with elasticity to grow. Final volumes confirmed during discovery.</b>
60.	5.2 Evaluation	Section 5.2 lists seven weighted evaluation criteria without point values or percentage weights. Will the State disclose the specific weighting, or confirm that 'Order of Importance' is the only weighting guidance?	<b>The State will not be disclosing the specific evaluation weighting; the 'Order of Importance' in Section 5.2 is the weighting guidance.</b>
61.	6.3.2 Submission Format	What is the State's target go-live date, and are there fixed milestones (e.g., RISE Summit, start of school year) that the project timeline must accommodate?	<b>The implementation timeline must accommodate the RISE Back to School Safety Summit. No fixed contractual go-live date is set; vendors may propose phased releases.</b>
62.	6.3.2 Submission Format	Section 6.3.2(a) requires one PDF containing 'all pages of this solicitation document.' Should the DIT Terms and Conditions (Attachment B) be included as a blank copy in the PDF, or acknowledged by reference?	<b>Attachment "B" (Information Technology Terms and Conditions) may be submitted as acknowledgement of the Attachment by reference.</b>

Question #	Solicitation Section	Vendor Question	State's Response
63.	6.3.3. Ariba Submission	If a vendor encounters Ariba upload issues in the final hour before the May 19, 2026, 2:00 PM deadline, is there a backup submission method (e.g., emergency email to the Contract Administrator)?	<b>No, there is no backup submission method if Vendors encounter Ariba upload issues in the final hours before the submission deadline. After the 2:00 PM EST deadline on May 19, 2026, no bids can be accepted in Ariba. The suggestion is do not wait until last day or hour to submit bids in case there are Ariba upload issues.</b>
64.	7.15 UAT and Remedies	Will UAT findings categorized as 'enhancements' (rather than defects against the stated requirements) be scoped as change requests at additional cost, or expected to be remediated within the base contract?	<b>The 8-week production acceptance testing period begins upon CFSS confirmation that all four portals are configured and the platform is functionally complete (post-implementation, prior to formal go-live announcement). UAT findings classified as defects against stated requirements shall be remediated within base contract; findings classified as enhancements (new functionality not in stated requirements) shall be scoped as change requests.</b>
65.	Attachment D: Cost Form	Is the 'Additional External User Accounts (per user)' line intended only for external content contributors beyond the initial 6 in Section 3.3.3, or does it also apply to training-portal registrants (potentially millions)? A per-user model may not be appropriate for the latter.	<b>This describes users outside of CFSS, within SBI or website builder that will have limited rights to make edits.</b>
66.	Attachment D: Cost Form	Will the State allow vendors to propose volume-based or tiered pricing that adjusts if actual registration and traffic exceed projected ranges, or must pricing be fully fixed for all five potential years regardless of adoption?	<b>Pricing is based on Firm-Fixed Pricing for the potential five (5) years.</b>
67.	Attachment G References	Will the State accept Attachment G references from Federal, DoD, higher-education or large K-12 school-district engagements, or must references be from state government / law enforcement clients specifically?	<b>References from federal, DoD, higher-education, or large K-12 school-district engagements may be submitted. References from state government or law enforcement clients are preferred. Per Q175, references must be from the prime Vendor only.</b>

Question #	Solicitation Section	Vendor Question	State's Response
68.	2.4 Contract Term	Section 2.4 states that the contract term is for 3 years with two option 1-year extensions. For Attachment D, should Vendors provide hosting and maintenance pricing for the initial 3-year team only, or for all 5 potential years?	<b>Vendors to provide pricing for all potential five (5) years</b>
69.	3.3.8 Accessibility	Section 3.3.8 requires compliance with WCAG 2.1 and Section 508. For the purposes of maintaining this compliance with regards to the uploaded content, will the Agency be responsible for ensuring the accessibility of the actual content they upload (e.g., providing closed captions for pre-recorded videos and accessible PDF documents)?	<b>Yes. The awarding agency (CFSS) is responsible for accessibility of content CFSS uploads after launch (closed captions on CFSS-produced videos, accessible PDFs, alt text, etc.), with vendor-provided tooling and guidance. The Vendor is responsible for accessibility of the platform, vendor-built templates, and content the Vendor creates or initially populates.</b>
70.	3.4.1	Will the State provide the Vendor with access to a non-production/sandbox Entra ID environment for development and testing purposes prior to user acceptance testing (UAT)?	<b>Yes — a non-production / sandbox Entra ID environment will be made available for development and testing prior to UAT.</b>
71.	7.15 UAT and Remedies	Section 7.15 outlines strict response and resolution time frames for system issues (e.g., 1-hour response for critical severe issues). Are these support and response times required 24x7x365, or are they based on standard state business hours (e.g., Monday-Friday, 8 AM - 5 PM EST), or a combination of these?	<b>Base support is business hours, Monday – Friday, 8:00 AM – 5:00 PM Eastern, excluding State holidays. Premium 24x7 support is an optional priced service. Severity 1 (production outage / security incident) shall have a 1-hour response 24x7x365 regardless of base support tier; resolution targets follow Section 7.15.</b>

Question #	Solicitation Section	Vendor Question	State's Response
72.	2.3 Summary of Problem Statement	The RFP notes requiring authentication for students, teachers, and law enforcement via their agency emails. Does CFSS have a process for on boarding users from these different groups to set them up for SSO/SAML authentication?	<b>Authentication model by portal: (1) Student Portal — unauthenticated public access, no PII collection, no account creation; (2) General Public Portal — unauthenticated public access, no PII collection; (3) Admin/Teacher/Support Staff Portal — email-based registration validated against approved LEA / charter school / education staff domains, MFA required for all users, manual approval by CFSS; (4) Law Enforcement Portal — email-based registration validated against approved law enforcement agency domains (.gov / .us), MFA required for all users, manual approval by CFSS. The earlier reference to MFA only for 'external contributors' is superseded by this clarification.</b>
73.	2.4 Contract Term	Could you share the estimated start date of the project to inform the development of the project timeline and budget?	<b>Estimated project start date is approximately 30 – 60 days following award and contract execution. Award is anticipated in summer 2026; vendors should plan timelines accordingly.</b>
74.	3.3.3 Identity and Access Management	Do you have a preferred tool for identity and access management? If not, do you want vendors to recommend a tool as part of our solution?	<b>Vendors shall recommend an identity and access management approach as part of their proposed solution. The State has Microsoft Entra ID for the limited CFSS administrator use case (Q19) but does not mandate an IdAM tool for the four portals' end users.</b>
75.	3.4.1 Platform Requirements	Is there prior WordPress or Drupal experience among the internal team or key stakeholders of this project?	<b>CFSS staff have limited prior CMS experience. Solution should be operable by users without specialized CMS training; embedded contextual guidance is preferred (see Q261).</b>
76.	3.4.3 Content Management Requirements	What survey tools do you use?	<b>CFSS currently uses Microsoft cloud tools (Microsoft Forms) for surveys.</b>
77.	3.4.4 Performance and Scalability	Do you have any data or analytics on the number of users/visitors the current page receives?	<b>No meaningful analytics are available — the current page is a Capitol Broadcasting–provided landing page only.</b>

Question #	Solicitation Section	Vendor Question	State's Response
78.	3.5.1 Website Design and UX	Does this project require any branding or design services for the CFSS initiative and/or website?	<b>Yes — CFSS has existing logos and a blue/white visual theme that must be applied. Two current logos will be provided. Vendors shall use these existing identity elements as the foundation; full brand discovery / new identity development is not in scope. Vendors should plan for content strategy, information architecture, page templates, navigation, plain-language editorial review, and accessibility tagging as part of base scope. Some content creation support is expected — see content authoring response.</b>
79.	3.5.2 Content Workflow and Collaboration	Does this project include the creation of new content for the website? Will you want the contractor to provide a copywriter to assist with this effort?	<b>The Vendor will provide initial website content, page structure, and information architecture, working with CFSS subject matter experts. CFSS will provide source material, training calendar information, and approved messaging. The Vendor shall include content entry, accessibility tagging, metadata, and basic copywriting in scope. Specialized training content (course material, video scripts, curricula) will be provided by CFSS. The Vendor shall propose ongoing content maintenance support as an option.</b>
80.	4.1 Offer Costs	Is there an anticipated budget range for this project?	<b>No, there is no anticipated budget range for this project.</b>
81.	5.2 Evaluation Criteria	Is there a target launch date for this website? Is there a hard launch date?	<b>The State has not set a fixed go-live date but the implementation timeline must accommodate the RISE Back to School Safety Summit (annually held in summer / pre-school-year) as a content driver. Vendors may propose phased releases.</b>
82.	6.3.2 Offer Organization	Please confirm that we need to include all pages of the RFP in our response and not just the items in the bulleted list on page 21.	<b>In accordance with 6.3.2, all content listed in a-h is to be included in the bid response.</b>

Question #	Solicitation Section	Vendor Question	State's Response
83.	7.11 Project Management	Will any content be migrated over from other locations, for instance from the current CFSS webpage: <a href="https://www.ncsbi.gov/Services/School-Safety/">https://www.ncsbi.gov/Services/School-Safety/</a> ? If there are other sites where content needs to be migrated from, could you share those sites?	<b>Yes — CFSS has existing logos and a blue/white visual theme that must be applied. Two current logos will be provided. Vendors shall use these existing identity elements as the foundation; full brand discovery / new identity development is not in scope. Vendors should plan for content strategy, information architecture, page templates, navigation, plain-language editorial review, and accessibility tagging as part of base scope. Some content creation support is expected — see content authoring response.</b>
84.	7.11 Project Management	Section 7.11 Project Management says: The Project Manager and key project team members identified above (in the Project Team Roster Table) must remain assigned to the project throughout implementation unless otherwise approved by the State. Any proposed changes to key personnel must be submitted in writing to the State for approval at least 30 days prior to the proposed change, along with qualifications of proposed replacement personnel. Are the Technical Lead and the Implementation Lead roles designated as Key Personnel?	<b>Yes — Technical Lead and Implementation Lead are designated as Key Personnel along with Project Manager. Substitution requires 30-day prior written notice and State approval per Section 7.11. The Project Manager shall participate in person at minimum at kickoff and major milestones; other meetings may be virtual per Section 7.12.</b>
85.	7.11 Project Management	Could you provide clarification on the difference in responsibilities between the Technical Lead and the Implementation Lead positions? We probably have different names for these roles so we want to properly map these to our project team composition. Could we recommend our own team roles and responsibilities that will better align with our team composition?	<b>Project Manager: overall delivery, schedule, status reporting, change control, stakeholder coordination. Technical Lead: solution architecture, security implementation, integrations, technical decisions, technical risk. Implementation Lead: content modeling, configuration, training delivery, UAT coordination, go-live readiness. Vendors may propose mapping to their internal team structure provided all responsibilities are covered and identified by name.</b>

Question #	Solicitation Section	Vendor Question	State's Response
86.	7.11 Project Management	A description or responsibilities was provided for the Project Manager position. Could a description be provided for the other roles listed in the Project Team Roster Table - Technical Lead and Implementation Lead?	<b>Project Manager: overall delivery, schedule, status reporting, change control, stakeholder coordination. Technical Lead: solution architecture, security implementation, integrations, technical decisions, technical risk. Implementation Lead: content modeling, configuration, training delivery, UAT coordination, go-live readiness. Vendors may propose mapping to their internal team structure provided all responsibilities are covered and identified by name.</b>
87.	7.11 Project Management	Are resumes required for this submission? If so, for which positions and where should they be placed in the response?	<b>Per the original response: resumes are not required for this submission.</b>
88.	2.3 Summary of Problem Statement	Section 2.3 states that the Student Portal and General Public Portal will be "unsecure," while Section 3.4.2 and Section 3.5.6 refer to four separate secure training portals and require safeguards for the Student Portal. Please clarify whether the Student and General Public portals should be public/open, authenticated, or secured through a different access model.	<b>Confirmed — Student Portal and General Public Portal shall be public/open (unsecured), no authentication or PII collection. Law Enforcement and Admin/Teacher portals require email-based authentication with MFA. See Q6, Q72, Q89, Q133, Q153, Q244.</b>
89.	3.4.2 Authentication and Access Control Requirements	Section 3.4.2 REQ-010b states that two portals must authenticate users via email-based registration, but the requirement text also references Law Enforcement, Admin/Teacher/Support Staff, Student, and General Public email types. Please confirm which portals require email-based authentication and whether personal email registration is required for the General Public Portal.	<b>Email-based authentication applies to the Law Enforcement and Admin/Teacher portals only. Personal email registration is not required for the General Public Portal — that portal is unsecured.</b>

Question #	Solicitation Section	Vendor Question	State's Response
90.	3.3.3 Identity and Access Management	For the Law Enforcement and Admin/Teacher/Support Staff portals, will the State provide approved agency, local education agency, charter school, and staff email domains for validation? If not, should the vendor propose a manual approval workflow for domains that cannot be automatically validated?	<b>CFSS will adjudicate all registration requests. The Vendor shall provide a master list / dashboard of approved users accessible to CFSS administrators, with workflow for approval, denial, suspension, and removal. CFSS does not maintain a pre-existing authoritative domain list; the approval-on-request model replaces blanket domain whitelisting. The Vendor is not required to research or maintain external domain lists.</b>
91.	3.4.2 Authentication and Access Control Requirements	Please clarify whether the Student Portal will collect any personally identifiable information from minors, allow account creation, track completion at an individual level, or provide only public content. This affects Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), consent, data minimization, and retention controls.	<b>The Student Portal will not collect any personally identifiable information from minors, will not allow account creation, will not track completion at an individual level, and will provide only public content (informational training and a video competition). FERPA, COPPA, consent, data minimization, and retention controls are addressed by not collecting any data.</b>
92.	3.5.6 Training Portal Specifications	Does CFSS require formal course completion records, certificates, quiz scores, continuing education units, or individual learner transcripts, or is portal usage and engagement reporting sufficient?	<b>The State requires pre-test and post-test capability for Law Enforcement and Admin/Teacher portal training. Vendors shall propose an LMS solution capable of pre/post assessments, individual completion tracking, basic quiz scoring, and exportable completion records for those two portals. Full SCORM/xAPI conformance, continuing education unit (CEU) tracking, and formal certificates are not required at launch but should be supported on the platform roadmap. The Student Portal hosts video content for a video competition only, with no individual progress tracking. The General Public Portal requires no LMS functionality.</b>

Question #	Solicitation Section	Vendor Question	State's Response
93.	3.4.2 & 3.5.6 Authentication and Access Control Requirements	Is the State expecting a content portal with training resources and registrations, or a full learning management system with enrollment, progress tracking, assessments, certificates, and learner records?	<b>The State requires pre-test and post-test capability for Law Enforcement and Admin/Teacher portal training. Vendors shall propose an LMS solution capable of pre/post assessments, individual completion tracking, basic quiz scoring, and exportable completion records for those two portals. Full SCORM/xAPI conformance, continuing education unit (CEU) tracking, and formal certificates are not required at launch but should be supported on the platform roadmap. The Student Portal hosts video content for a video competition only, with no individual progress tracking. The General Public Portal requires no LMS functionality.</b>
94.	2.3 Summary of Problem Statement	Section 2.3 provides large addressable populations for capacity planning. Does the State have estimated Year 1, Year 2, and Year 3 adoption or registered-user targets for each portal to support more precise infrastructure sizing and cost estimates?	<b>Anticipated registration volumes are not estimated at this time; addressable populations in Section 2.3 are upper bounds, not targets. Vendors shall propose tiered pricing assumptions.</b>
95.	2.3 & 3.4.4 Summary of Problem Statement	Please define any expected peak traffic scenarios, such as press events, statewide school safety incidents, summit registration launches, or grant announcements, including desired concurrent user assumptions if available.	<b>Expected peak traffic occurs prior to and following the RISE Back to School Safety Summit, prior to the start of the school year, and following statewide school safety incidents. Concurrent user assumptions are not estimated; vendors shall propose tiered scaling assumptions.</b>
96.	3.3.6 Data Migration	How many existing pages, documents, videos, forms, event records, dashboards, and training resources should be migrated into the new site and portals? Please confirm whether the vendor is responsible for remediating existing documents for accessibility.	<b>There is minimal content migration. The current <a href="https://ncsbi.gov/Services/School-Safety">ncsbi.gov/Services/School-Safety</a> landing page (Capitol Broadcasting) is the only existing source. CFSS's training calendar from the prior <a href="https://cfssnc.gov">cfssnc.gov</a> website shall be migrated. No bulk document, video, or dashboard migration is required. Vendors are not responsible for accessibility remediation of legacy content not migrated.</b>

Question #	Solicitation Section	Vendor Question	State's Response
97.	3.3.8 Accessibility	Will the State accept a Voluntary Product Accessibility Template (VPAT) or accessibility conformance report for the CMS and hosting components, supplemented by project-specific accessibility testing results for the delivered website?	<b>VPAT / Accessibility Conformance Report is required at offer submission. A solution VPAT (CMS / hosting platform) plus a project-specific accessibility testing report at go-live is acceptable. Continuous automated accessibility scanning is preferred but not required; manual testing at minimum quarterly is required.</b>
98.	3.3.4 Integration Approach	Are Power BI, YouTube, Whova, Eventbrite, Google Workspace, and survey tools already licensed and approved by the State, or should the vendor include any licensing, configuration, and accessibility review assumptions in the cost proposal?	<b>The following are currently licensed and in use by CFSS / NC SBI and will be made available for integration: Microsoft 365 (including Teams), YouTube (public), Whova, Eventbrite, Google Workspace (where used by CFSS), Microsoft Forms / Microsoft cloud surveys. Power BI licensing model for embedding shall be confirmed during discovery; if Power BI Embedded capacity licensing is required for the proposed embedding model, the Vendor shall include this in the cost proposal as a separately identified line item. Domain / DNS, SSL certificates, and email/transactional messaging services associated with the new platform shall be included in Vendor pricing.</b>
99.	3.3.3 Identity and Access Management	Will NC SBI provide access to a development/test Microsoft Entra ID tenant and technical contacts during implementation for SAML 2.0 or OpenID Connect integration testing?	<b>Entra ID authentication is for the 2-3 CFSS administrative users only. End users of the Law Enforcement and Admin/Teacher portals authenticate via the email-based registration model with MFA described above, not via Entra ID. NC SBI will provide Entra ID application registration, metadata, test accounts, attribute mapping, and a coordination point for the limited Entra ID integration. A non-production / sandbox Entra ID environment will be made available prior to UAT.</b>

Question #	Solicitation Section	Vendor Question	State's Response
100.	3.2.2 Solutions Not Hosted on State Infrastructure	For NIST 800-53 Moderate alignment, will the State accept the hosting provider's FedRAMP authorization or SOC 2 Type II report plus the completed VRAR, or is a solution-specific third-party assessment required prior to award?	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>
101..	3.3.5 Disaster Recovery and Business Continuity	Please confirm required Recovery Point Objective and Recovery Time Objective targets. If none are mandated, may vendors propose commercially reasonable targets with optional enhanced recovery pricing?	<b>Recovery Point Objective (RPO) ≤ 24 hours and Recovery Time Objective (RTO) ≤ 4 hours apply to the full production environment, including all four portals and the CMS-managed embedded content references. Embedded third-party content (Power BI, YouTube, Google Workspace) availability is governed by those providers. Documented manual runbook with tested annual failover is acceptable; fully automatic failover is not required. Off-site, immutable backups isolated from the primary hosting environment are required to defend against ransomware / destructive attack scenarios.</b>

Question #	Solicitation Section	Vendor Question	State's Response
102.	3.4.1 Platform Requirements	REQ-005 requires a 99.9% uptime service level agreement with documented remedies. Does the State have required service credit language or minimum remedies, or may the vendor propose its standard remedies?	<b>99.9% uptime SLA is required, measured monthly excluding scheduled maintenance windows. The Vendor's standard service credit schedule is acceptable as the documented remedy for non-compliance, provided credits are meaningful (minimum 5% of monthly recurring fees per 0.1% below SLA, escalating). Specific liquidated damages are not required. Auto-scaling shall absorb traffic surges typical of post-event and pre-school-year periods without service degradation; specific surge multipliers are not mandated, but the Vendor's proposed scaling capacity will be evaluated.</b>
103.	3.5.4 Support Services	Please clarify required support hours for routine support and emergency support, including whether 24/7 coverage is required for Severity 1 outages or security incidents.	<b>Base support is business hours, Monday – Friday, 8:00 AM – 5:00 PM Eastern, excluding State holidays. Premium 24x7 support is an optional priced service. Severity 1 (production outage / security incident) shall have a 1-hour response 24x7x365 regardless of base support tier; resolution targets follow Section 7.15.</b>
104.	3.3.1 Architecture Diagrams	Can the required network and technology stack diagrams use vendor-standard notation and redact sensitive provider-specific details where necessary for security, while still showing all required logical components?	<b>Required at offer submission: completed VRAR, current SOC 2 Type II report (or executive summary if confidential, with full report available under NDA prior to award), evidence of FedRAMP Moderate authorization for the proposed hosting platform, and a current third-party penetration test attestation (full report under NDA acceptable). VPAT is required at offer submission. Detailed network diagrams may use vendor-standard notation and may redact provider-specific operational details, provided all logical components and integration points are shown.</b>

Question #	Solicitation Section	Vendor Question	State's Response
105.	3.4.5 Training Requirements	The RFP references training for two to three internal users. Please confirm whether this includes only content editors and administrators or also Regional School Safety Specialists and external contributors.	<b>Training is for 2-3 internal CFSS users (administrators / content editors). External contributors and Regional School Safety Specialists are not included in the formal training count; they will receive contextual / role-based platform guidance as part of normal operations. Embedded role-based, LMS-style training and contextual guidance within the platform is preferred over external documentation alone.</b>
106.	3.5.2 Content Workflow and Collaboration	Should CFSS require a single centralized approval workflow for all content or separate approval paths by program area, portal, and content type?	<b>Separate editorial workflow paths are required by program area, portal, and content type. Vendor shall propose a workflow capable of supporting at minimum: public content workflow, restricted training portal workflow, and law enforcement portal workflow, each with editor → reviewer → approver stages. CFSS will define final reviewer / approver assignments during discovery.</b>
107.	4.1 & Attachment D Offer Costs	Attachment D appears to require itemized offer costs. Should vendors separate costs by implementation, hosting, maintenance, support, training, optional enhancements, and each option year?	<b>Vendors are to submit pricing in accordance with the Attachment Form D: Sections listed: Implementation (1.1), Hosting, Maintenance, Support and Training (1.2), Optional Enhancements (1.4) and Option Years (1.3).</b>

Question #	Solicitation Section	Vendor Question	State's Response
108.	3.4.2 Authentication and Access Control Requirements	Section 2.3 states "The law enforcement portal and teacher portal will use two factor authentication as mentioned in 3.3.3". However, Section 3.3.3 only mentions MFA for external contributors (up to 6 users). Does the State require MFA for the estimated 230,000 end-users of the law enforcement and teacher portals? If so, should the vendor include the cost of an MFA solution (e.g., SMS, Authenticator app) for these users in the cost proposal?	<b>Authentication model by portal: (1) Student Portal — unauthenticated public access, no PII collection, no account creation; (2) General Public Portal — unauthenticated public access, no PII collection; (3) Admin/Teacher/Support Staff Portal — email-based registration validated against approved LEA / charter school / education staff domains, MFA required for all users, manual approval by CFSS; (4) Law Enforcement Portal — email-based registration validated against approved law enforcement agency domains (.gov / .us), MFA required for all users, manual approval by CFSS. The earlier reference to MFA only for 'external contributors' is superseded by this clarification.</b>
109.	3.3.3 Identity and Access Management	For email domain validation (e.g., .gov, .us, and specific school district domains) required for self-registration, will the State provide and maintain the master list of approved domains, or is the vendor expected to research, build, and maintain this list?	<b>CFSS will adjudicate all registration requests. The Vendor shall provide a master list / dashboard of approved users accessible to CFSS administrators, with workflow for approval, denial, suspension, and removal. CFSS does not maintain a pre-existing authoritative domain list; the approval-on-request model replaces blanket domain whitelisting. The Vendor is not required to research or maintain external domain lists.</b>
110.	3.4.2 Authentication and Access Control Requirements	The requirement mentions "live/scheduled virtual training sessions with registration capabilities." Will the vendor need to provide and host the actual web-conferencing/streaming software (e.g., Zoom, Webex), or will the CMS simply be required to link out to/integrate with an existing State-owned webinar platform?	<b>Live and scheduled virtual training sessions will be hosted by CFSS using Microsoft Teams (externally accessible). The platform shall integrate registration only — calendar publishing, registration capture, reminders, and basic attendance reporting. The Vendor is not required to provide a web conferencing platform.</b>

Question #	Solicitation Section	Vendor Question	State's Response
111.	3.4.3 Content Management Requirements	REQ-013 states the solution must support embedded video content from YouTube. Must the solution <i>also</i> provide native video hosting and streaming capabilities with associated storage for the "pre-recorded video courses" mentioned in REQ-010d, or will all videos be hosted on YouTube/external platforms?	<b>Pre-recorded video for the Student Portal video competition and General Public Portal will primarily be hosted via YouTube embeds. The platform shall support YouTube embeds, embedded Teams recordings, and limited native video where required. Native large-scale video hosting and streaming with associated CDN storage is not in baseline scope; vendors may propose as optional.</b>
112.	3.5.6 Training Portal Specifications	The RFP mentions delivering training materials, video courses, and tracking "training completion." Is the State seeking a Learning Management System (LMS) with SCORM compliance and individual progress tracking, or simply a CMS that restricts page access and tracks basic page views/activity?	<b>The State requires pre-test and post-test capability for Law Enforcement and Admin/Teacher portal training. Vendors shall propose an LMS solution capable of pre/post assessments, individual completion tracking, basic quiz scoring, and exportable completion records for those two portals. Full SCORM/xAPI conformance, continuing education unit (CEU) tracking, and formal certificates are not required at launch but should be supported on the platform roadmap. The Student Portal hosts video content for a video competition only, with no individual progress tracking. The General Public Portal requires no LMS functionality.</b>
113.	3.2.2 Solutions Not Hosted on State Infrastructure	The RFP states that the system will manage data classified as Low Risk (Public) data, but mandates NIST 800-53 Moderate security controls. Can the State confirm that NIST Moderate is strictly required for this project, as this significantly impacts the underlying infrastructure and hosting costs compared to a Low baseline?	<b>Data classification is Low Risk (Public). NIST SP 800-53 Moderate baseline controls are firm and required regardless of classification, due to the Solution's exposure to law enforcement users, school personnel, and minors. The Solution shall not process Criminal Justice Information (CJI) or PII of minors beyond minimal account registration data for authenticated portals (Law Enforcement and Admin/Teacher portals only).</b>
114.	3.4.1 Platform Requirements	Has the State considered leveraging NC Digital Commons and their Drupal infrastructure, templates, and components for this project?	<b>The State has not designated NC Digital Commons for this procurement. Vendors may propose its use but it is not required and confers no preference.</b>

Question #	Solicitation Section	Vendor Question	State's Response
115.	3.4.1 Platform Requirements	RFP describes both a public-facing informational website AND four separate training portals. Are the training portals subsections within the main website, or standalone applications/microsites? Affects architecture, URL structure, and cost.	<b>The four portals shall be implemented as four sections under a single 'Training Portals' tab redirecting to the appropriate authentication or public landing page, on a single multi-site / multi-tenant CMS configuration (e.g., WordPress Multisite or Drupal multi-site). A single CMS back end with separate front ends is not acceptable as proposed in Q134 — a single integrated multi-site solution is required. Audience-specific menus and content listings are required; full distinct branding per portal is not required.</b>
116.	2.3 & 3.4.2 Summary of Problem Statement	Student Portal is described as “unsecure” yet must comply with FERPA and COPPA. What student data will be collected/stored? Will students create accounts? What age groups? COPPA applies to children under 13 — if middle schoolers (grades 6–8) are included, parental consent workflows may be required.	<b>Confirmed — no student data will be collected or stored. The Student Portal is informational only (videos, training resources, video competition entries managed externally). No accounts created. COPPA parental consent workflows are not required because no PII is collected from any user.</b>
117.	2.3 & 3.4.2 Summary of Problem Statement	Cost form includes “Website Design and Development.” Is the vendor responsible for initial content creation, visual design (branding, custom graphics), and copywriting, or only for setting up the CMS infrastructure and templates?	<b>The Vendor will provide initial website content, page structure, and information architecture, working with CFSS subject matter experts. CFSS will provide source material, training calendar information, and approved messaging. The Vendor shall include content entry, accessibility tagging, metadata, and basic copywriting in scope. Specialized training content (course material, video scripts, curricula) will be provided by CFSS. The Vendor shall propose ongoing content maintenance support as an option.</b>

Question #	Solicitation Section	Vendor Question	State's Response
118.	4.1 & Attachment D: Offer Costs	Does CFSS expect a built-in webinar/virtual classroom capability, or is embedding third-party tools (Zoom, Teams) sufficient? Registration capabilities imply more than simple embedding.	<b>Live and scheduled virtual training sessions will be hosted by CFSS using Microsoft Teams (externally accessible). The platform shall integrate registration only — calendar publishing, registration capture, reminders, and basic attendance reporting. The Vendor is not required to provide a web conferencing platform.</b>
119.	3.4.2 Authentication and Access Control Requirements	What are the expected concurrent user peaks? Does the State have any baseline analytics from the current single page?	<b>The State does not have historical analytics for the existing single landing page (currently provided by Capitol Broadcasting; no meaningful traffic data available). Adoption rate targets and concurrent user counts for Years 1, 3, and 5 are not available. Addressable populations stated in Section 2.3 are upper bounds. Vendors shall propose tiered pricing and capacity assumptions; recurring pricing should assume FedRAMP Moderate hosting with standard business-hours support, with 24x7 / premium support priced as an optional service. Anticipated peak conditions occur prior to and following large events such as the RISE Back to School Safety Summit, and prior to the start of the school year.</b>
120.	2.3 & 3.4.4 Summary of Problem Statement	Embedding Power BI via iframe in a public-facing portal requires specific licensing (Power BI Embedded). Does CFSS already have Power BI Embedded licenses, or should the vendor include this in their cost proposal?	<b>Power BI Embedded licensing model shall be confirmed during discovery. Where Power BI Embedded capacity licensing is required for the proposed embedding model in public-facing portals, the Vendor shall include this in the cost proposal as a separately identified line item. CFSS / NC SBI's existing Power BI Pro licenses do not extend to anonymous public embedding.</b>

Question #	Solicitation Section	Vendor Question	State's Response
121.	3.3.4 Integration Approach	For the Law Enforcement and Admin/Teacher portals, how many distinct email domains need to be whitelisted? ~500 law enforcement agencies + 115+ LEAs + 200+ charter schools represent significant domain management effort.	<b>CFSS will adjudicate all registration requests. The Vendor shall provide a master list / dashboard of approved users accessible to CFSS administrators, with workflow for approval, denial, suspension, and removal. CFSS does not maintain a pre-existing authoritative domain list; the approval-on-request model replaces blanket domain whitelisting. The Vendor is not required to research or maintain external domain lists.</b>
122.	2.4.2 & 3.3.3 Authentication and Access Control Requirements	Section 2.3 mentions "high-level functionality expected for each solution release into production." Does the State expect a phased rollout (e.g., main site first, portals later), and if so, what is the expected timeline for full deployment?	<b>The State has not set a fixed go-live date but the implementation timeline must accommodate the RISE Back to School Safety Summit (annually held in summer / pre-school-year) as a content driver. Vendors may propose phased releases.</b>
123.	2.3 Summary of Problem Statement	Does CFSS or NC SBI have an existing brand style guide, design system, or visual identity standards that must be applied to the new website?	<b>Yes — CFSS has existing logos and a blue/white visual theme that must be applied. Two current logos will be provided. Vendors shall use these existing identity elements as the foundation; full brand discovery / new identity development is not in scope. Vendors should plan for content strategy, information architecture, page templates, navigation, plain-language editorial review, and accessibility tagging as part of base scope. Some content creation support is expected — see content authoring response.</b>
124.	3.5.1 Website Design and User Experience	Are there any expected storage limits for uploaded documents and video content, or bandwidth constraints the vendor should plan for?	<b>No specific storage limits or bandwidth constraints are mandated. Vendor shall propose appropriate sizing with elasticity to grow. See Q59 for estimated initial volumes.</b>
125.	General	Please confirm offerors may use a title page and cover letter.	<b>Yes, an offeror may include a title page and cover letter with their bid submission.</b>
126.	General	What is the expected budget range for this initiative?	<b>There is no estimated budget for this project initiative.</b>
127.	2.6 Contract Type	The Contract Type listed is Definite Quantity Contract. Please confirm this will be structured as fixed price.	<b>This is a Fixed Price Contract</b>

Question #	Solicitation Section	Vendor Question	State's Response
128.	3.0 Requirements & Specifications	What pain points are you experiencing with the current approach to sharing resources, training, and information?	<b>Current pain point: lack of a dedicated, consolidated digital space for school safety resources, training materials, event information, and audience-specific content. Existing presence is a single landing page, which cannot support the four-audience training and resource model CFSS requires.</b>
129.	3.0 Requirements & Specifications	The RFP requests a hosted CMS platform and four portals, but provides limited detail on discovery, requirements validation, and functional design. Should vendors assume that the awarded contractor is expected to lead discovery, information architecture, user experience design, content model definition, and release planning as part of the base scope?	<b>Yes, the awarded contractor is expected to lead discovery, information architecture, user experience design, content model definition, and release planning as part of the base scope. Stakeholder participation should plan for representatives from CFSS (primary), NC SBI IT (security, identity, infrastructure review), CFSS leadership (executive sponsor), and select educator and law enforcement advisors as available. Plan for approximately 8-12 stakeholders across reviews; usability testing with target audiences (students, teachers, law enforcement) is expected — vendor should include recruitment plan and methods.</b>
130.	3.0 Requirements & Specifications	Please clarify whether CFSS requires the portals to provide Learning Management System (LMS) capabilities (e.g., tracking enrollment, completion, and user progress), or if the requirement is limited to secure content management and distribution of materials.	<b>The State requires pre-test and post-test capability for Law Enforcement and Admin/Teacher portal training. Vendors shall propose an LMS solution capable of pre/post assessments, individual completion tracking, basic quiz scoring, and exportable completion records for those two portals. Full SCORM/xAPI conformance, continuing education unit (CEU) tracking, and formal certificates are not required at launch but should be supported on the platform roadmap. The Student Portal hosts video content for a video competition only, with no individual progress tracking. The General Public Portal requires no LMS functionality.</b>

Question #	Solicitation Section	Vendor Question	State's Response
131.	3.0 Requirements & Specifications	Will the vendor be responsible for creating the training content, or just building the portal while CFSS provides and manages the content? If so, what is the length or duration of time of each training course? How many training courses for each audience are expected each year?	<b>CFSS will author training content. The Vendor is responsible for the content delivery platform, LMS proposal, structuring of pre/post tests within the LMS, and providing publishing tools. The Vendor is not responsible for video production, animation, scripting, slide remediation, course narration, or copywriting of training content.</b>
132.	3.0 Requirements & Specifications	Please confirm whether the State anticipates collecting personally identifiable information beyond basic account data, given the referenced FERPA and COPPA requirements.	<b>Confirmed — no PII collection beyond minimal account registration data (email address) for the Law Enforcement and Admin/Teacher portals. No PII collection from minors. Refer to Q91, Q116, Q152, Q159.</b>
133.	3.0 Requirements & Specifications	The RFP states that the Student portal will be "unsecure", but later describes access as "accessible by students", and again on page 11 in table 3.4.2 describes as "four secure portals". Can CFSS clarify if the state portal will require student authentication, and the intended means for that authentication?	<b>Authentication model by portal: (1) Student Portal — unauthenticated public access, no PII collection, no account creation; (2) General Public Portal — unauthenticated public access, no PII collection; (3) Admin/Teacher/Support Staff Portal — email-based registration validated against approved LEA / charter school / education staff domains, MFA required for all users, manual approval by CFSS; (4) Law Enforcement Portal — email-based registration validated against approved law enforcement agency domains (.gov / .us), MFA required for all users, manual approval by CFSS. The earlier reference to MFA only for 'external contributors' is superseded by this clarification.</b>

Question #	Solicitation Section	Vendor Question	State's Response
134.	3.0 Requirements & Specifications	CFSS has asked for four distinct portals. Given that the RFP states that training resources and content be published to multiple portals, will CFSS consider an architecture that is a single CMS back end, with separate front ends?	<b>The four portals shall be implemented as four sections under a single 'Training Portals' tab redirecting to the appropriate authentication or public landing page, on a single multi-site / multi-tenant CMS configuration (e.g., WordPress Multisite or Drupal multi-site). A single CMS back end with separate front ends is not acceptable as proposed in Q134 — a single integrated multi-site solution is required. Audience-specific menus and content listings are required; full distinct branding per portal is not required.</b>
135.	3.0 Requirements & Specifications	The RFP references third-party event registration tools such as Whova and Eventbrite and also references live/scheduled training sessions with registration capabilities. Please clarify whether vendors are expected to provide native registration and attendance-management functionality within the solution, or only support integration/embedding with third-party registration platforms.	<b>Vendors shall provide integration / embedding support for third-party event registration platforms (Whova, Eventbrite). Native registration / waitlist / capacity / reminders functionality within the platform is not required.</b>
136.	3.3.1 Architecture Diagrams	Among the items specified as being part of the "ONE PDF" to be submitted as our proposal, is item 6.3.2(d) Architecture Diagrams. Section 3.3.1 of the RFP refers to the NCDIT Vendor Engagement Website which expresses a preference for vendors to submit architecture diagrams via MS Visio other native or editable diagram formats. Does this supersede the above requirement for a single PDF and should the architecture diagrams be submitted as a separate (preferably Visio) file attachment?	<b>Architecture diagrams shall be included within the single PDF proposal per Section 6.3.2. Vendors may additionally submit native editable diagram formats (Visio, etc.) as supplemental files; the PDF inclusion remains required.</b>

Question #	Solicitation Section	Vendor Question	State's Response
137.	General	The RFP provides estimated addressable populations for the four portals and references surge conditions during high-profile events. Please provide any available estimates for peak concurrent users, expected monthly traffic, storage volumes, or anticipated growth assumptions vendors should use for infrastructure sizing and cost proposals.	<b>The State does not have historical analytics for the existing single landing page (currently provided by Capitol Broadcasting; no meaningful traffic data available). Adoption rate targets and concurrent user counts for Years 1, 3, and 5 are not available. Addressable populations stated in Section 2.3 are upper bounds. Vendors shall propose tiered pricing and capacity assumptions; recurring pricing should assume FedRAMP Moderate hosting with standard business-hours support, with 24x7 / premium support priced as an optional service. Anticipated peak conditions occur prior to and following large events such as the RISE Back to School Safety Summit, and prior to the start of the school year.</b>
138.	6.3.2 Offer Organization	The proposal preparation instructions indicate that all items listed in 6.3.2(a) are to be submitted in a single PDF file. However, it is unclear whether the remaining items in 6.3.2, (b) through (h), are also to be included in the single PDF. Are these actually supposed to be stand-alone files and not part of the "ONE PDF?" Please clarify.	<b>The items listed in 6.3.2 (b – h) are also to be included in the single PDF file.</b>
139.	Attachment B	Will Offerors be allowed to provide redlines to the General Terms and Conditions with their submissions?	<b>Yes, offerors may provide redlines to the General Terms and Conditions with their submissions.</b>
140.	Attachment B	Will Subcontractors included in Vendor proposal be considered to have prior written consent?	<b>The State Contract is with the primary Vendor not the subcontractor. That is at the discretion of the Vendor to determine prior to bid submission.</b>
141.	Attachment B	How soon after the execution of the Subcontract agreement shall Vendor provide complete copies to the State?	<b>Subcontractor agreements must be provided with Vendor's bid submission.</b>
142.	Ariba Sourcing Site	Requirement states, "Vendor shall upload a Signed and Completed version of the solicitation document found in Section 3 of the Sourcing Event here. Vendor is advised to confirm that it has reviewed and provided all requested information as applicable." Is NCSBI requesting offerors to sign and submit page 1 of the solicitation or the entire solicitation?	<b>In accordance with Section 6.3.2, Vendor is to submit all pages listed there.</b>

Question #	Solicitation Section	Vendor Question	State's Response
143.	Ariba Sourcing Tool	Requirement states, "Vendor shall upload file(s) that contains its complete offer with all applicable contents as specified in the Proposal Content and Organization section of the solicitation." Are offerors to upload their entire proposal including a) signed execution page, attachments A through H and b) through h) (listed on page 21) in one PDF?	<b>Yes, offerors are to upload their entire proposal in one PDF.</b>
144.	General	Given the short time frame between the release of CFSS answers to bidder's questions and the current due date for bidder responses, will CFSS provide a one-week extension for responses?	<b>There will not be an extension for responses.</b>
145.	2.1 Introduction	Please confirm that a managed WordPress or Drupal platform hosted by a third-party platform provider is acceptable if the prime vendor remains responsible for implementation, support, and compliance with all RFP requirements.	<b>Both Drupal and WordPress are acceptable and will be evaluated equally, provided all mandatory security, hosting, accessibility, and portal requirements are met. There is no internal preference. Managed WordPress / Drupal platforms (e.g., Pantheon, Acquia, WP Engine) hosted by a third-party platform provider are acceptable if FedRAMP Moderate, U.S. data residency, and U.S. personnel requirements are met, and the prime Vendor remains responsible for implementation, support, and compliance. The State has not standardized on NC Digital Commons for this procurement; vendors may propose, but it is not required.</b>

Question #	Solicitation Section	Vendor Question	State's Response
146.	3.2.2 Solutions Not Hosted on State Infrastructure	Please confirm whether NIST 800-53 Moderate compliance may be demonstrated through the proposed solution's platform or managed hosting environment, such as a FedRAMP-authorized managed CMS or platform service, together with vendor controls for implementation and operations.	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>
147.	3.2.2 Solutions Not Hosted on State Infrastructure	Please clarify whether a FedRAMP Moderate authorization for a managed CMS, PaaS, or SaaS hosting platform will satisfy the preferred third-party assessment requirement, provided the authorization applies to the proposed production environment.	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>

Question #	Solicitation Section	Vendor Question	State's Response
148.	3.2.2 Solutions Not Hosted on State Infrastructure	Please confirm which security assessment materials are required at offer submission versus prior to contract award. If detailed SOC 2, FedRAMP, penetration test, or vulnerability reports are confidential, may vendors submit executive summaries, attestation letters, or controlled-access documentation?	<b>Required at offer submission: completed VRAR, current SOC 2 Type II report (or executive summary if confidential, with full report available under NDA prior to award), evidence of FedRAMP Moderate authorization for the proposed hosting platform, and a current third-party penetration test attestation (full report under NDA acceptable). VPAT is required at offer submission. Detailed network diagrams may use vendor-standard notation and may redact provider-specific operational details, provided all logical components and integration points are shown.</b>
149.	3.2.2 Solutions Not Hosted on State Infrastructure	For a proposed solution involving a prime vendor, platform provider, and subcontractors, should the VRAR be submitted as one consolidated solution-level assessment or should separate VRAR materials be provided for each major service provider?	<b>VRAR shall be submitted as one consolidated solution-level assessment covering the prime Vendor's controls and the inheritance/responsibility model for the platform provider and any subcontractors. Separate VRARs are not required, but the consolidated VRAR must clearly identify which controls are inherited, shared, or fully owned by each party.</b>
150.	3.3.1 Architecture Diagrams	Please clarify the expected scope of the required Network Architecture and Technology Stack diagrams. Should diagrams include only vendor-managed components, or should they also depict integrations with State systems such as Microsoft Entra ID, Power BI, DNS, email, and third-party content tools?	<b>Architecture diagrams shall depict all integrations with State systems including Microsoft Entra ID (CFSS administrator authentication only), Power BI, DNS, email, and third-party content tools, in addition to vendor-managed components. Vendor-standard notation is acceptable; sensitive provider-specific operational details may be redacted.</b>

Question #	Solicitation Section	Vendor Question	State's Response
151.	3.4.1 & Attachment F	Please confirm whether the United States location requirement applies only to hosting infrastructure or also to all vendor and subcontractor personnel with administrative access, support access, or access to State data.	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>
152.	3.2.2, 2.3 & 3.4.2 Solutions Not Hosted on State Infrastructure	Section 3.2.2 classifies the solution data as Low Risk Public, while Sections 2.3 and 3.4.2 reference student users and FERPA/COPPA considerations. Please confirm the data classification and whether the solution is expected to collect, store, or process student personally identifiable information.	<b>Confirmed — data classification is Low Risk (Public). The Solution shall not collect, store, or process student PII. NIST 800-53 Moderate controls are required regardless, due to the operational context.</b>
153.	2.3, 3.3.3 & 3.4.2 Summary of Problem Statement	9. Please clarify which of the four training portals must be authenticated. Section 2.3 states the Student Portal and General Public Portal will be unsecured, while Section 3.3.3 describes four separate secure training portals, and REQ-010b lists email-based registration for all four portals.	<b>Authentication model by portal: (1) Student Portal — unauthenticated public access, no PII collection, no account creation; (2) General Public Portal — unauthenticated public access, no PII collection; (3) Admin/Teacher/Support Staff Portal — email-based registration validated against approved LEA / charter school / education staff domains, MFA required for all users, manual approval by CFSS; (4) Law Enforcement Portal — email-based registration validated against approved law enforcement agency domains (.gov / .us), MFA required for all users, manual approval by CFSS. The earlier reference to MFA only for 'external contributors' is superseded by this clarification.</b>

Question #	Solicitation Section	Vendor Question	State's Response
154.	2.3, 3.3.3 & 3.4.2 Summary of Problem Statement	Please clarify which user populations require MFA. Is MFA required only for internal CFSS staff and external content contributors, or also for law enforcement, admin/teacher/support staff, student, and general public portal users?	<b>Authentication model by portal: (1) Student Portal — unauthenticated public access, no PII collection, no account creation; (2) General Public Portal — unauthenticated public access, no PII collection; (3) Admin/Teacher/Support Staff Portal — email-based registration validated against approved LEA / charter school / education staff domains, MFA required for all users, manual approval by CFSS; (4) Law Enforcement Portal — email-based registration validated against approved law enforcement agency domains (.gov / .us), MFA required for all users, manual approval by CFSS. The earlier reference to MFA only for 'external contributors' is superseded by this clarification.</b>
155.	3.3.3 & 3.4.2 Identity and Access Management	11. Will the State provide and maintain the authoritative domain lists for law enforcement agencies, school districts, charter schools, and educational institutions, or should the vendor include domain discovery, verification, and ongoing maintenance in scope?	<b>CFSS will adjudicate all registration requests. The Vendor shall provide a master list / dashboard of approved users accessible to CFSS administrators, with workflow for approval, denial, suspension, and removal. CFSS does not maintain a pre-existing authoritative domain list; the approval-on-request model replaces blanket domain whitelisting. The Vendor is not required to research or maintain external domain lists.</b>
156.	3.3.3 & 3.5.6 3.3.3 & 3.4.2 Identity and Access Management	Please state the preferred registration and provisioning model for each portal, such as self-registration with email-domain validation, self-registration with manual approval, invitation-only access, or a hybrid approach.	<b>Self-registration with email submission, plus manual approval by CFSS, plus MFA enrollment for the Law Enforcement and Admin/Teacher portals. Student and General Public portals are unsecured (no registration).</b>
157.	2.3 & 3.5.6 Summary of Problem Statement	The RFP provides addressable user populations for each portal. Please provide the State's expected year-one registered users, monthly active users, and peak concurrent users for each portal to support infrastructure sizing and pricing.	<b>Anticipated registration volumes are not estimated at this time; addressable populations in Section 2.3 are upper bounds, not targets. Vendors shall propose tiered pricing assumptions.</b>

Question #	Solicitation Section	Vendor Question	State's Response
158.	2.3 & 3.4.4 Summary of Problem Statement	To support accurate pricing for managed CMS hosting, CDN, WAF/DDoS, backup/DR, MFA, support, and scalable portal operations, please provide the State's estimated Monthly Unique Visitors (MUV) for the public website and estimated monthly unique authenticated users / monthly active users (MUA) for each of the four portals for Year 1 and steady state. Please also provide expected monthly page views or requests, peak concurrent users during high-profile school safety events, and expected storage/download or media-delivery volume. If these estimates are not available, may vendors submit tiered pricing assumptions, and should base recurring pricing assume a FedRAMP Moderate hosting environment and standard support, with 24x7/premium support priced as an optional service?	<b>The State does not have historical analytics for the existing single landing page (currently provided by Capitol Broadcasting; no meaningful traffic data available). Adoption rate targets and concurrent user counts for Years 1, 3, and 5 are not available. Addressable populations stated in Section 2.3 are upper bounds. Vendors shall propose tiered pricing and capacity assumptions; recurring pricing should assume FedRAMP Moderate hosting with standard business-hours support, with 24x7 / premium support priced as an optional service. Anticipated peak conditions occur prior to and following large events such as the RISE Back to School Safety Summit, and prior to the start of the school year.</b>
159.	3.4.2 & 3.5.6 Authentication and Access Control Requirements	For the Student Portal, should vendors assume that the solution must avoid collecting student PII where possible, or should vendors include capabilities for student account profiles, parental consent workflows, and student training records?	<b>Vendors shall assume the Solution must avoid collecting student PII. Student account profiles, parental consent workflows, and student training records are NOT required and shall not be implemented for the Student Portal.</b>
160.	3.5.6 Training Portal Specifications	Please clarify the expected learning and training management capabilities. Are vendors expected to provide course progress tracking, completion status, certificates, quizzes, transcripts, continuing education records, or only portal usage and content engagement analytics?	<b>The State requires pre-test and post-test capability for Law Enforcement and Admin/Teacher portal training. Vendors shall propose an LMS solution capable of pre/post assessments, individual completion tracking, basic quiz scoring, and exportable completion records for those two portals. Full SCORM/xAPI conformance, continuing education unit (CEU) tracking, and formal certificates are not required at launch but should be supported on the platform roadmap. The Student Portal hosts video content for a video competition only, with no individual progress tracking. The General Public Portal requires no LMS functionality.</b>

Question #	Solicitation Section	Vendor Question	State's Response
161.	3.3.3 & 3.4.2 Identity and Access Management	Please confirm whether the external contributors referenced as up to six users are content contributors only and are separate from the larger training portal user populations.	<b>Confirmed — the up to six external contributors are content contributors only. They are separate from the Law Enforcement and Admin/Teacher portal end users.</b>
162.	3.1.5 & 3.3.4 Enterprise Licensing	Please identify which third-party tools and licenses will be provided by the State, including Power BI, YouTube, Whova, Eventbrite, survey tools, Google Workspace, analytics, domain/DNS, SSL certificates, and email/transactional messaging services, versus which should be included in vendor pricing.	<b>The following are currently licensed and in use by CFSS / NC SBI and will be made available for integration: Microsoft 365 (including Teams), YouTube (public), Whova, Eventbrite, Google Workspace (where used by CFSS), Microsoft Forms / Microsoft cloud surveys. Power BI licensing model for embedding shall be confirmed during discovery; if Power BI Embedded capacity licensing is required for the proposed embedding model, the Vendor shall include this in the cost proposal as a separately identified line item. Domain / DNS, SSL certificates, and email/transactional messaging services associated with the new platform shall be included in Vendor pricing.</b>
163.	3.3.4 & 3.5.3 Integration Approach	Are there State restrictions or preferences for analytics tools, cookies, tracking scripts, IP address collection, or third-party analytics services such as Google Analytics?	<b>Google Analytics is acceptable for this site. Vendor shall confirm cookie banner and privacy notice meet North Carolina and FERPA / COPPA expectations given the audience includes minors (even though no PII is collected). LMS-specific user progress data combined with Google Analytics satisfies the user activity tracking requirement.</b>

Question #	Solicitation Section	Vendor Question	State's Response
164.	3.3.8 & 5.2 Accessibility	Please confirm the required accessibility conformance level. Should vendors design, develop, and test to WCAG 2.1 Level AA in addition to Section 508?	<b>WCAG 2.1 Level AA conformance is required, in addition to Section 508. The Vendor is responsible for accessibility of: the platform itself, vendor-built templates, vendor-developed components, and content the Vendor creates or initially populates. CFSS is responsible for accessibility of content CFSS uploads after launch (closed captions on CFSS-produced videos, accessible PDFs, alt text on uploaded images), with vendor-provided tooling and guidance.</b>
165.	3.3.8 & 5.2 Accessibility	Please confirm when a VPAT or Accessibility Conformance Report is required: with the offer, prior to award, at go-live, or after final accessibility testing of the implemented solution.	<b>VPAT / Accessibility Conformance Report is required at offer submission. A solution VPAT (CMS / hosting platform) plus a project-specific accessibility testing report at go-live is acceptable. Continuous automated accessibility scanning is preferred but not required; manual testing at minimum quarterly is required.</b>
166.	3.3.6 & 2.3 Data Migration	Although Section 3.3.6 states no data migration is required, should vendors include effort to recreate, reorganize, or copy existing CFSS content, documents, links, and resources from the current NC SBI page into the new website?	<b>There is minimal content migration. The current <a href="https://ncsbi.gov/Services/School-Safety">ncsbi.gov/Services/School-Safety</a> landing page (Capitol Broadcasting) is the only existing source. CFSS's training calendar from the prior <a href="https://cfssnc.gov">cfssnc.gov</a> website shall be migrated. No bulk document, video, or dashboard migration is required. Vendors are not responsible for accessibility remediation of legacy content not migrated.</b>

Question #	Solicitation Section	Vendor Question	State's Response
167.	3.5.1 Website Design and User Experience	Will the State provide CFSS and NC SBI brand guidelines, logos, style requirements, approved imagery, and content standards, or should vendors include brand discovery and visual design development in scope?	<b>Yes — CFSS has existing logos and a blue/white visual theme that must be applied. Two current logos will be provided. Vendors shall use these existing identity elements as the foundation; full brand discovery / new identity development is not in scope. Vendors should plan for content strategy, information architecture, page templates, navigation, plain-language editorial review, and accessibility tagging as part of base scope. Some content creation support is expected — see content authoring response.</b>
168.	General	Please provide the desired implementation schedule or target go-live date following award, if one exists. If no target date exists, may vendors propose a phased launch timeline?	<b>The State has not set a fixed go-live date but the implementation timeline must accommodate the RISE Back to School Safety Summit (annually held in summer / pre-school-year) as a content driver. Vendors may propose phased releases.</b>
169.	7.15 Special Terms & Conditions	Please clarify when the eight-week production acceptance testing period begins. Does it begin after completion of training, after go-live, after all four portals are configured, or after another milestone?	<b>The 8-week production acceptance testing period begins upon CFSS confirmation that all four portals are configured and the platform is functionally complete (post-implementation, prior to formal go-live announcement). UAT findings classified as defects against stated requirements shall be remediated within base contract; findings classified as enhancements (new functionality not in stated requirements) shall be scoped as change requests.</b>
170.	7.15 Special Terms & Conditions	Severity 1 issues require a one-hour response time. Does this requirement imply 24x7 support for Severity 1 incidents, or may vendors provide business-hours support with emergency escalation unless optional premium 24x7 support is purchased?	<b>Base support is business hours, Monday – Friday, 8:00 AM – 5:00 PM Eastern, excluding State holidays. Premium 24x7 support is an optional priced service. Severity 1 (production outage / security incident) shall have a 1-hour response 24x7x365 regardless of base support tier; resolution targets follow Section 7.15.</b>

Question #	Solicitation Section	Vendor Question	State's Response
171.	3.4.4 Performance and Scalability Requirements	Please define how the average page load time requirement of three seconds or less will be measured, including test locations, representative pages, authenticated versus unauthenticated pages, cached versus uncached traffic, and expected load conditions.	<b>The 3-second average page-load requirement shall be measured: (a) for representative authenticated and unauthenticated public-facing pages, (b) using synthetic monitoring from at least one U.S. East and one U.S. Central monitoring location, (c) under typical broadband network conditions, (d) for first-byte and document-complete metrics excluding third-party embedded content load time (Power BI, Google Workspace, video). Vendors shall propose the specific page templates to be measured.</b>
172.	3.4.1 Platform Requirements	Please clarify whether the required 99.9% uptime SLA must include service credits, specific remedies, or only documented remedies for non-compliance.	<b>99.9% uptime SLA is required, measured monthly excluding scheduled maintenance windows. The Vendor's standard service credit schedule is acceptable as the documented remedy for non-compliance, provided credits are meaningful (minimum 5% of monthly recurring fees per 0.1% below SLA, escalating). Specific liquidated damages are not required. Auto-scaling shall absorb traffic surges typical of post-event and pre-school-year periods without service degradation; specific surge multipliers are not mandated, but the Vendor's proposed scaling capacity will be evaluated.</b>
173.	Attachment B	May the prime vendor use subcontractor or teaming partner experience and references to satisfy Attachment G, provided those subcontractors will perform material portions of the resulting contract?	<b>No, the prime Vendor may not use subcontractor or teaming partner experience or references to satisfy Attachment G.</b>
174.	Attachment G	Please confirm whether references may include federal, state, local, education, nonprofit, or commercial customers, and whether references must use the same proposed CMS platform and hosting environment.	<b>References may include federal, state, local, education, nonprofit, or commercial customers. References are not required to use the same proposed CMS platform and hosting environment, but vendors should highlight where comparable platforms or scopes were delivered.</b>

Question #	Solicitation Section	Vendor Question	State's Response
175.	Attachment G	For Attachment G, must the three references be from the prime vendor only, or may references be submitted for the proposed solution team, including platform, hosting, accessibility, or implementation partners?	<b>The references must be from the prime Vendor only.</b>
176.	Attachment H	Section 7.2 refers to Attachment I, while the RFP includes Attachment H as the Financial Review Form. Please confirm that Attachment H is the required Financial Review Form. For privately held companies without audited financial statements, please confirm whether a CPA statement as described in Section 7.2(b) is acceptable.	<b>Vendors shall submit a completed Attachment H Financial Review Form along with internally prepared financial statements sufficient to demonstrate financial stability and ability to perform the contract. Audited financial statements are not required for this solicitation. The State may request additional financial information or clarification as necessary (such as a written statement from an independent CPA) to evaluate vendor responsibility.</b>
177.	Attachment B	Please confirm whether the 1.75% E-Procurement transaction fee should be built into vendor pricing, since the fee may not be stated or invoiced as a separate item.	<b>The 1.75% e-Procurement Fee does not apply to service contracts.</b>
178.	Attachment D	For usage-based services such as hosting, CDN, WAF/DDoS, MFA, storage, bandwidth, support, and portal users, may vendors include capacity assumptions, usage tiers, or optional pricing for growth beyond stated assumptions?	<b>For usage-based services, use the stated assumptions</b>
179	7.12 Meetings	Please clarify the expected number of in-person meetings or training sessions in Raleigh, NC, if any, so vendors can include all travel costs in the proposed pricing.	<b>The Vendor's Project Manager shall attend at minimum, in person; per Section 7.12, other meetings may be virtual if necessary</b>
180.	7.11 Project Management	Please confirm the correct project point of contact and email address for post-award project coordination. Page 26 lists an email address with a comma in the domain and references a Grant Management System Project Point of Contact.	<b>Per Section 7.11, Phillip Broughton is the Project Point of Contact.</b>

Question #	Solicitation Section	Vendor Question	State's Response
181.	3.4.3 Content Management Requirements	Are commercial plugins, modules, or extensions for WordPress or Drupal permitted if they are documented, maintained, patched, and included in the proposed security and accessibility approach?	<b>Commercial WordPress / Drupal plugins, modules, and extensions are permitted provided they are: actively maintained by the publisher, included in the Vendor's documented patching cadence, covered by the Vendor's security and accessibility approach, and disclosed in the architecture submission. Abandoned or unmaintained modules are not acceptable.</b>
182.	3.2.2 & 3.5.4 Solutions Not Hosted on State Infrastructure	Please confirm the expected cadence for vulnerability scanning, penetration testing, security patching, and reporting during the contract term.	<b>Vulnerability scanning shall be performed at minimum monthly and after any significant change. Annual third-party penetration testing is required, with results provided to the State. Critical and High severity vulnerabilities (CVSS 7.0+) shall be remediated within 15 calendar days; Medium within 30 days. Zero-day vulnerabilities affecting the production environment shall be triaged within 24 hours and mitigated/patched within 72 hours, or compensating controls applied. Modern security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy) are required at launch.</b>
183.	3.3.7 & 3.5.6 Application Management	Please provide any required data retention periods for user accounts, audit logs, content change logs, training completion records, portal analytics, and support records.	<b>Audit logs, authentication logs, content change logs, and administrative action logs shall be retained for a minimum of 365 days online and 3 years total (online + archived). Logs must be tamper-evident and exportable to the State on request. Media library files shall have version control and activity tracking equivalent to page/post edits.</b>

Question #	Solicitation Section	Vendor Question	State's Response
184.	3.3.4 & 3.5.5 Integration Approach	Are vendors permitted to use commercial AI-assisted tools for development, testing, accessibility support, search, content recommendations, or content drafting, if no State data is entered into public AI tools without approval?	<b>Vendors may use commercial AI-assisted tools for development, testing, accessibility support, search, content recommendations, or content drafting, provided no State data is entered into public AI tools without State approval, and provided AI use is disclosed. NC SBI's interim AI usage policy prohibits CJI/PII/LES entry into any AI tool. Preference will not be given to vendors offering AI-driven backend capabilities (per Q256); AI use is permitted but not preferred.</b>
185.	General	Given the short interval between the written questions deadline (April 28, 2026), anticipated State responses/RFP Addendum (May 5, 2026), and offer opening deadline (May 19, 2026), will the State extend the final offer submission deadline by two weeks to allow vendors sufficient time to incorporate the State's responses, finalize architecture, security, staffing, and pricing assumptions, and prepare a complete best-value proposal?	<b>No extension to the May 19, 2026, 2:00 PM EST submission deadline.</b>
186.	4.1 Offer Costs & Attachment D	Does the State have an approved implementation budget, target budget range, or not-to-exceed amount for this procurement, including Year 1 implementation and recurring hosting, maintenance, and support? If the State cannot disclose a budget, please confirm vendors should propose a best-value solution and may include optional or tiered pricing to show cost/capability tradeoffs.	<b>No, there is no implementation or targeted budget range. Vendors are to submit proposal pricing in accordance with the cost alignments within Attachment D: Cost Form.</b>
187.	4.1 Offer Costs & Attachment D	Please confirm how optional services or usage tiers will be evaluated under the Total Cost of Ownership factor. Should optional 24x7 support, premium traffic tiers, increased portal adoption, additional content services, additional training services, and increased storage/bandwidth be included in the evaluated price or priced separately as optional services?	<b>The optional services in Attachment D is to be evaluated for informational purposes and not factored into Total Cost.</b>

Question #	Solicitation Section	Vendor Question	State's Response
188.	2.3 & 3.4.4 Summary of Problem Statement	Please provide any available historical analytics for the existing NC SBI School Safety page and related third-party platforms, including monthly users, page views, resource downloads, video views, event registration volume, form submissions, and traffic spikes during school-safety incidents or high-profile events. If these analytics are unavailable, may vendors submit pricing based on stated assumptions?	<b>No historical analytics are available beyond the existing Capitol Broadcasting landing page. Vendors may submit pricing based on stated assumptions and tiered models.</b>
189.	2.3 & 3.5.1 Summary of Problem Statement	How many State stakeholders should vendors assume will participate in discovery, design reviews, content reviews, technical/security reviews, user acceptance testing, and final acceptance? Please identify anticipated stakeholder groups, such as CFSS, NC SBI, NCDIT, law enforcement, educators, students/parents, communications, legal/privacy, and executive sponsors.	<b>Yes, the awarded contractor is expected to lead discovery, information architecture, user experience design, content model definition, and release planning as part of the base scope. Stakeholder participation should plan for representatives from CFSS (primary), NC SBI IT (security, identity, infrastructure review), CFSS leadership (executive sponsor), and select educator and law enforcement advisors as available. Plan for approximately 8-12 stakeholders across reviews; usability testing with target audiences (students, teachers, law enforcement) is expected — vendor should include recruitment plan and methods.</b>
190.	7.11 Project Management	Does the State have expectations for minimum vendor roles or dedicated staffing levels beyond Project Manager, Technical Lead, and Implementation Lead? Should vendors identify a UX/Design Lead, Content Strategist, Accessibility Lead, Security/Compliance Lead, Data/Analytics Lead, Training Lead, and Support Lead? Are part-time or shared resources acceptable during implementation and steady-state operations?	<b>Beyond the three Key Personnel, vendors should plan for a UX/Design Lead, Accessibility Lead, and Security/Compliance Lead at minimum. Part-time and shared resources are acceptable for non-Key Personnel during implementation and steady-state.</b>

Question #	Solicitation Section	Vendor Question	State's Response
191.	2.3 & 3.5.1 Summary of Problem Statement	Does the State expect formal discovery or user research with target audiences before information architecture and design are finalized? If yes, please clarify the expected methods and scale, such as stakeholder interviews, user interviews, surveys, workshops, card sorting, tree testing, usability testing, and whether the State will recruit/provide participants or vendors should include recruitment and facilitation in scope.	<b>Yes, formal discovery with target audiences is expected before information architecture and design are finalized, including stakeholder interviews, user interviews, light usability testing, and at least one card sort / tree test for navigation. Vendor shall include recruitment and facilitation in scope; CFSS will assist with introductions to law enforcement and educator participants.</b>
192.	3.5.1 & 3.5.6 Website Design and User Experience	Please clarify expected design deliverables, including the number of initial design concepts, homepage mockups, subpage mockups, mobile/tablet states, portal-specific templates, design system or component library, revision rounds, and whether clickable prototypes are expected before build.	<b>Initial design and build target: estimated 6-10 distinct page templates, 8-12 content types, and 30-60 initial content pages across the public site and four portals. Vendors should plan accordingly; final scope confirmed during discovery. Two design concepts and 1-2 rounds of revisions are expected; clickable prototypes are preferred.</b>
193.	3.5.1 & 2.3 Website Design and User Experience	Should vendors assume CFSS has existing brand guidelines and visual identity, or should vendors include brand discovery and creation/refinement of colors, typography, imagery style, iconography, design tokens, and editorial tone? Should the website align primarily with NC SBI, CFSS, NC.gov, or a new CFSS identity?	<b>Yes — CFSS has existing logos and a blue/white visual theme that must be applied. Two current logos will be provided. Vendors shall use these existing identity elements as the foundation; full brand discovery / new identity development is not in scope. Vendors should plan for content strategy, information architecture, page templates, navigation, plain-language editorial review, and accessibility tagging as part of base scope. Some content creation support is expected — see content authoring response.</b>

Question #	Solicitation Section	Vendor Question	State's Response
194.	2.3 & 3.4.3 Summary of Problem Statement	Please clarify whether the vendor is expected to provide content strategy and content design services, including information architecture, taxonomy, content models, page templates, navigation labels, plain-language rewriting, metadata, search optimization, calls-to-action, and audience-specific content paths, or only configure the CMS and load State-provided content.	<b>The Vendor will provide initial website content, page structure, and information architecture, working with CFSS subject matter experts. CFSS will provide source material, training calendar information, and approved messaging. The Vendor shall include content entry, accessibility tagging, metadata, and basic copywriting in scope. Specialized training content (course material, video scripts, curricula) will be provided by CFSS. The Vendor shall propose ongoing content maintenance support as an option.</b>
195.	2.3, 3.3.4, 3.5.2 & 3.5.2 Summary of Problem Statement	Please provide an estimated initial content inventory for launch, including the number of public pages, portal pages, training items, PDFs, Word/PowerPoint documents, videos, Power BI dashboards, forms, surveys, event registration embeds, Google Workspace embeds, and downloadable resources. If an inventory is unavailable, may vendors provide scoped assumptions and pricing options?	<b>Initial design and build target: estimated 6-10 distinct page templates, 8-12 content types, and 30-60 initial content pages across the public site and four portals. Vendors should plan accordingly; final scope confirmed during discovery. Two design concepts and 1-2 rounds of revisions are expected; clickable prototypes are preferred.</b>
196.	3.4.3 & 3.5.2	Who will author, edit, approve, and publish initial website and portal content? Please clarify whether the State will provide final approved copy/assets before implementation, or whether the vendor should include copywriting, editing, content entry, accessibility tagging, metadata creation, and content QA in scope.	<b>The Vendor will provide initial website content, page structure, and information architecture, working with CFSS subject matter experts. CFSS will provide source material, training calendar information, and approved messaging. The Vendor shall include content entry, accessibility tagging, metadata, and basic copywriting in scope. Specialized training content (course material, video scripts, curricula) will be provided by CFSS. The Vendor shall propose ongoing content maintenance support as an option.</b>

Question #	Solicitation Section	Vendor Question	State's Response
197.	2.3, 3.4.2 & 3.5.6 Summary of Problem Statement	For the Student Portal, should vendors support different grade or age bands, reading levels, content warnings, parent/guardian considerations, moderated content, or student-specific plain-language standards? Who will approve student-facing and age-appropriate content?	<b>All Student Portal content will be posted by CFSS staff and shall be appropriate for the grade 6–12 audience. Vendor is not responsible for age-band content variants, reading-level adjustment, or moderated content. CFSS approves all student-facing content.</b>
198.	3.4.2, 3.4.5 & 3.5.6 Authentication and Access Control Requirements	Please confirm whether vendors are responsible only for the portal framework and content delivery capabilities, or also for producing and structuring training courses. Should scope include video production/editing, captions/transcripts, slide/document remediation, quizzes, completion certificates, continuing education records, course sequencing, SCORM/xAPI support, and training completion reporting?	<b>CFSS will authorize training content. The Vendor is responsible for the content delivery platform, LMS proposal, structuring of pre/post tests within the LMS, and providing publishing tools. The Vendor is not responsible for video production, animation, scripting, slide remediation, course narration, or copywriting of training content.</b>
199.	3.3.8 & 3.4.3 Accessibility	For State-provided documents, videos, dashboards, forms, and embedded third-party content, who is responsible for accessibility remediation, including PDF tagging, alt text, captions, transcripts, keyboard testing, color contrast, and VPAT/Accessibility Conformance Report documentation? Will accessible source files be provided by the State?	<b>Vendor is responsible for accessibility of the platform, vendor-built templates, and any content the Vendor creates or initially populates. CFSS will create training content and is responsible for accessibility of CFSS-uploaded materials (PDF tagging, alt text, captions, transcripts) using vendor-provided tooling. Vendor shall provide guidance and accessible source templates. VPAT / ACR is required at offer submission per Q219.</b>
200.	3.5.4 & Attachment D	Please provide the expected ongoing monthly support volume after launch, including content updates, user provisioning/deprovisioning requests, help desk tickets, portal administration requests, security/patch events, and analytics/reporting requests. If unavailable, may vendors propose support tiers with included request volumes and rates for overages?	<b>Annual enhancement / change request budget shall be priced as a not-to-exceed pool of hours (vendor proposes; the State suggests planning for approximately 200 – 400 hours per year). The State prefers a fixed annual fee for proactive patching, updates, and routine enhancement; T&amp;M billing is acceptable for discrete change requests beyond the pool.</b>

Question #	Solicitation Section	Vendor Question	State's Response
201.	General	Are there fixed calendar drivers for implementation, such as the school year start, RISE Back to School Safety Summit, grant cycles, training cohorts, or public safety campaigns? Should vendors propose phased releases by public site and individual portals, or should they assume a single full go-live?	<b>Calendar drivers: the school year start (August) and the RISE Back to School Safety Summit (summer) are the primary scheduling anchors. Vendors may propose phased releases (public site first, then portals) or a single full go-live. The training calendar is the most time-sensitive content item.</b>
202.	5.2 & 6.3.2 Evaluation Criteria	Are HUB, NCSBE, veteran-owned, service-disabled veteran-owned, or other supplier diversity certifications considered in evaluation, reporting, or subcontracting goals for this procurement? If so, please identify the applicable certification program, required forms, and whether out-of-state certifications will be accepted.	<b>No, supplier diversity certifications are not considered in this evaluation.</b>
203.	General	Are there any required platforms or systems for the training modules (e.g., LMS like Canvas), or are vendors able to recommend/build the solution?	<b>The State requires pre-test and post-test capability for Law Enforcement and Admin/Teacher portal training. Vendors shall propose an LMS solution capable of pre/post assessments, individual completion tracking, basic quiz scoring, and exportable completion records for those two portals. Full SCORM/xAPI conformance, continuing education unit (CEU) tracking, and formal certificates are not required at launch but should be supported on the platform roadmap. The Student Portal hosts video content for a video competition only, with no individual progress tracking. The General Public Portal requires no LMS functionality.</b>
204.	General	Are there existing systems (CMS, LMS, authentication tools) that the new website must integrate with?	<b>No existing CMS, LMS, or authentication tool integrations are required beyond those described in this Addendum (Entra ID for CFSS administrators only; embedded Power BI; YouTube; Microsoft Forms; Whova / Eventbrite; Microsoft Teams).</b>

Question #	Solicitation Section	Vendor Question	State's Response
205.	General	Do you have a preferred hosting environment or security requirements (e.g., state IT standards, data residency, accessibility compliance beyond ADA)?	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>
206.	General	Will content be provided for both the website and training modules, or is content development/support expected as part of the scope?	<b>The Vendor will provide initial website content, page structure, and information architecture, working with CFSS subject matter experts. CFSS will provide source material, training calendar information, and approved messaging. The Vendor shall include content entry, accessibility tagging, metadata, and basic copywriting in scope. Specialized training content (course material, video scripts, curricula) will be provided by CFSS. The Vendor shall propose ongoing content maintenance support as an option.</b>
207.	General	What are the top 3 actions you want users to take on the site (e.g., complete training, access resources, report concerns)?	<b>Top three user actions in priority order are (1) access resources, (2) complete training, (3) report concerns</b>
208.	General	Are there examples of websites or training platforms you feel are effective or aligned with your vision?	<b><a href="https://kycss.org/">https://kycss.org/</a> has been provided as a reference of the desired feel; confirmation pending. Vendors are encouraged to bring additional examples of effective state-level school safety platforms.</b>

Question #	Solicitation Section	Vendor Question	State's Response
209.	General	Will the email protected training modules require progress tracking, certifications, or reporting capabilities?	<b>Email-protected training portals (Law Enforcement and Admin/Teacher) shall require pre/post test capability and individual completion tracking — see Q49, Q92, Q112. The Student Portal video competition does not require individual progress tracking; only aggregated submission tracking external to the portal.</b>
210.	General	Hosting Preference: Given the robust server-related requirements in the VRAR, does the State prefer the vendor to host the solution on State-managed infrastructure to ensure the State maintains direct responsibility for server-level compliance (SSL, scaling, backups, etc.)?	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>
211.	General	Editable File Policy: To maintain high security standards, will the State permit the conversion of all Word/PPT documents to PDF for public distribution?	<b>Yes — the State permits conversion of Word and PowerPoint documents to PDF for public distribution to reduce attack surface. Editable formats may be hosted via secure external links per Q212.</b>
212.	General	Cloud Links: If editable documents are strictly required, would the State approve the use of secure, external links (e.g., Google Docs) for downloading these files rather than hosting vulnerable file types directly on the web server?	<b>Yes — secure external links to editable documents (e.g., Google Docs, SharePoint links) for download are approved in lieu of hosting editable file formats directly on the web server, where editable formats are required.</b>

Question #	Solicitation Section	Vendor Question	State's Response
213.	General	Administrative Logging: Beyond standard WordPress page revisions and login timestamps, what specific "administrative actions" must be logged?	<b>Administrative actions to be logged include, at minimum: user creation / modification / deletion, role assignment changes, content publishing, content deletion, system configuration changes, plugin / module install or update, security setting changes, login successes and failures, MFA enrollment changes, and data export operations.</b>
214.	General	Media Versioning: Is version control and activity tracking required for files in the media library, or is tracking limited to page and post edits?	<b>Yes — version control and activity tracking are required for files in the media library, with at minimum 10 prior versions retained and timestamped activity logs.</b>
215.	General	User Analytics: Will standard Google Analytics, combined with LMS-specific user progress data, satisfy the requirement for tracking user activity?	<b>Google Analytics is acceptable for this site. Vendor shall confirm cookie banner and privacy notice meet North Carolina and FERPA / COPPA expectations given the audience includes minors (even though no PII is collected). LMS-specific user progress data combined with Google Analytics satisfies the user activity tracking requirement.</b>
216.	General	Level of Compliance: Is the State requiring 100% WCAG compliance (including audio descriptions for every image), or is the priority focused on high-contrast design, keyboard navigability, alt-text, and closed captioning?	<b>WCAG 2.1 Level AA conformance is required, in addition to Section 508. The Vendor is responsible for accessibility of: the platform itself, vendor-built templates, vendor-developed components, and content the Vendor creates or initially populates. CFSS is responsible for accessibility of content CFSS uploads after launch (closed captions on CFSS-produced videos, accessible PDFs, alt text on uploaded images), with vendor-provided tooling and guidance.</b>
217.	General	Accessibility Tools: Is the inclusion of a front-end accessibility plugin (allowing users to manually adjust contrast and font size) a required feature for the build?	<b>A front-end accessibility plugin allowing users to manually adjust contrast and font size is required. State-uploaded documents that can be rendered as PDF or as a Google Doc external link (where editable formats are required) is acceptable, in lieu of hosting Word / PowerPoint files directly.</b>

Question #	Solicitation Section	Vendor Question	State's Response
218.	General	Data Centralization: To streamline user experience and data management, would the State prefer the use of integrated survey tools (e.g., Gravity Forms) to keep all submissions stored directly on the site, rather than using external third-party platforms?	<b>Surveys may be implemented natively in the platform or embedded from third-party services. Microsoft Forms (Microsoft cloud) is the State's primary tool. Either integrated forms (e.g., Gravity Forms) keeping submissions on-platform, or embedded Microsoft Forms, is acceptable. Vendor shall propose both options and identify trade-offs.</b>
219.	3.3.8 Accessibility	Is submission of a VPAT required at offer submittal or acceptable upon award?	<b>VPAT is required with offer submission.</b>
220.	Attachment D: Cost Form	Are optional services included in Attachment D evaluated strictly for informational purposes, or do they factor into Total Cost of Ownership evaluation scoring?	<b>he optional services in Attachment D is to be evaluated for informational purposes and not factored into Total Cost.</b>
221.	7.2 Financial Statements	Section 7.2 references an Attachment I – can the State confirm this should be Attachment H or should there be an additional attachment?	<b>The reference to the Financial Review Form is for Attachment H.</b>
222.	7.2 Financial Statements	Section 7.2(b) provides that for privately held vendors without certified audited financial statements, a written statement from the company's certified public accountant addressing financial condition and stability may be submitted, and further states that the State may accept evidence of financial stability other than financial statements at its discretion. For a privately held small business, would submission of a CPA letter addressing financial sufficiency and ability to perform the contract be considered responsive without submission of Attachment H (Financial Review Form), provided the letter addresses the State's intent under Section 7.2?	<b>Vendors shall submit a completed Attachment H Financial Review Form along with internally prepared financial statements sufficient to demonstrate financial stability and ability to perform the contract. Audited financial statements are not required for this solicitation. The State may request additional financial information or clarification as necessary (such as a written statement from an independent CPA) to evaluate vendor responsibility.</b>
223.	General	Can the State share the budget or approximate ceiling for this effort?	<b>There was no budget or approximate ceiling established for this project.</b>

Question #	Solicitation Section	Vendor Question	State's Response
224.	3.2.2 Solutions Not Hosted on State Infrastructure	Who owns hosting and liability?	<b>Hosting and operational responsibility rests with the Vendor under the resulting contract. Data ownership remains with the State at all times. Breach response, indemnification, and limitation of liability are governed by Attachment B (IT Terms and Conditions); Vendors may submit redlines per Question 139. The Vendor is responsible for breach notification to the State within 24 hours of confirmed incident, per Attachment B.</b>
225.	2.3 Problem of Summary Statement	How distinct do the four user groups need to be (fully separate portals vs. Role-based within one system)?	<b>The four portals shall be implemented as four sections under a single 'Training Portals' tab redirecting to the appropriate authentication or public landing page, on a single multi-site / multi-tenant CMS configuration (e.g., WordPress Multisite or Drupal multi-site). A single CMS back end with separate front ends is not acceptable as proposed in Q134 — a single integrated multi-site solution is required. Audience-specific menus and content listings are required; full distinct branding per portal is not required.</b>
226.	2.3 Problem of Summary Statement	Will users require authentication for all portals, or certain sections only?	<b>Authentication is required for all access to the Law Enforcement and Admin/Teacher portals (no anonymous browsing of those portals). Student and General Public portals are fully unauthenticated. Refer to Q6, Q72, Q88, Q244.</b>

Question #	Solicitation Section	Vendor Question	State's Response
227.	3.2.2 Solutions Not Hosted on State Infrastructure	What documentation or certification will be required from the vendor for hosting and security?	<b>Required at offer submission: completed VRAR, current SOC 2 Type II report (or executive summary if confidential, with full report available under NDA prior to award), evidence of FedRAMP Moderate authorization for the proposed hosting platform, and a current third-party penetration test attestation (full report under NDA acceptable). VPAT is required at offer submission. Detailed network diagrams may use vendor-standard notation and may redact provider-specific operational details, provided all logical components and integration points are shown.</b>
228.	2.1 Purpose of RFP	Is there any internal experience with WordPress or Drupal that would lead to a preference for either platform?	<b>No internal preference for WordPress vs Drupal. Either platform is acceptable.</b>
229.	3.4.1 Platform Requirements	Should the solution be expected to operate as standalone applications or can it be a single multi-site setup?	<b>The four portals shall be implemented as four sections under a single 'Training Portals' tab redirecting to the appropriate authentication or public landing page, on a single multi-site / multi-tenant CMS configuration (e.g., WordPress Multisite or Drupal multi-site). A single CMS back end with separate front ends is not acceptable as proposed in Q134 — a single integrated multi-site solution is required. Audience-specific menus and content listings are required; full distinct branding per portal is not required.</b>
230.	General	Reviewing the contracts already in place, it appears that the Bureau already has a contract with Microsoft for services.	<b>Yes — NC SBI has Microsoft enterprise agreements (Microsoft 365 GCC G5, Entra ID, Teams). Microsoft tooling is the State standard for productivity, identity for CFSS administrators, and live virtual training delivery (Teams). The awarded Vendor is not provided Microsoft licensing for end users; integration with Entra ID for the limited CFSS administrative use case is required.</b>

Question #	Solicitation Section	Vendor Question	State's Response
231.	3.4.1 Platform Requirements	Is there a preferred cloud infrastructure provider (AWS, Azure, etc.)?	<b>No required cloud provider. Solution must meet FedRAMP Moderate hosting and U.S. data residency requirements. The State has Microsoft enterprise agreements but is not making Azure tenancy, Microsoft 365 services, or Azure hosting credits available to the awarded Vendor for this engagement, except for the limited Entra ID integration described elsewhere.</b>
232.	3.5.6 Training Portal Specifications	Are there existing CDN, WAF, or DDoS services already contracted by the State that could be used?	<b>No existing State CDN, WAF, or DDoS services are designated for this procurement. The Vendor shall provide CDN, WAF, and DDoS protection as part of the proposed FedRAMP Moderate hosting solution.</b>
233.	3.4.1 Platform Requirements	How will NIST 800-53 compliance be validated in practice (audit, documentation review, inherited controls)?	<b>Required at offer submission: completed VRAR, current SOC 2 Type II report (or executive summary if confidential, with full report available under NDA prior to award), evidence of FedRAMP Moderate authorization for the proposed hosting platform, and a current third-party penetration test attestation (full report under NDA acceptable). VPAT is required at offer submission. Detailed network diagrams may use vendor-standard notation and may redact provider-specific operational details, provided all logical components and integration points are shown.</b>

Question #	Solicitation Section	Vendor Question	State's Response
234.	3.4.1 Platform Requirements	Will the State accept platform-level inheritance (FedRAMP-authorized hosting + hardened CMS), or must the CMS layer itself be certified?	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>
235.	3.4.2 Authentication and Access Control Requirements	Please clarify the Entra ID authentication usage. The RFP states this is for 2-3 users? Is this just for the admin of the system, or will there only need to be 2-3 users that use the Entra ID system? The project requirements imply that all agency and school staff will require the use of the Entra ID system. Is Entra ID intended only for CFSS administrative users, while the four training portals use email-based authentication for end users?	<b>Entra ID authentication is for the 2-3 CFSS administrative users only. End users of the Law Enforcement and Admin/Teacher portals authenticate via the email-based registration model with MFA described above, not via Entra ID. NC SBI will provide Entra ID application registration, metadata, test accounts, attribute mapping, and a coordination point for the limited Entra ID integration. A non-production / sandbox Entra ID environment will be made available prior to UAT.</b>
236.	3.5.6 Training Portal Specifications	What is the expected user lifecycle process (manual approval vs. automated provisioning or a combination)? What is the State's expected user lifecycle process for portal users— fully self-service registration with automated domain validation, manual administrator approval, invitation-only provisioning, or a hybrid model that varies by portal?	<b>User lifecycle is self-registration with CFSS manual approval, active maintenance via the user master list, and automatic deactivation when a user's government / school / agency email becomes invalid (verified via periodic email validation, at minimum annually). When a user is no longer employed by their school system or law enforcement agency, the email-based access ceases to function and the account shall be flagged for CFSS review.</b>

Question #	Solicitation Section	Vendor Question	State's Response
237.	General	Is multi-lingual support required?	<b>Multi-lingual support is not required at launch. The platform should support future Spanish-language content addition without re-platforming.</b>
238.	General	Will the State provide brand guidelines, existing content, or prior user research, or should the vendor budget for brand development, content creation, and discovery activities as part of the engagement?	<b>Two existing CFSS logos and a blue / white visual theme will be provided. Vendors should budget for: light brand application work, content discovery and creation, information architecture, and stakeholder engagement. Full new identity development is not in scope.</b>
239.	7.15 Special Terms and Conditions	Is usability testing with customers (students, teachers, law enforcement) expected?	<b>Yes — usability testing with target audiences (students, teachers, law enforcement) is expected. Vendor shall include recruitment plan and methods; CFSS will assist with introductions where possible.</b>
240.	2.6 Contract Type	Would the state prefer fully itemized pricing or a fixed bid with annual hosting costs?	<b>This is a Fixed-Price Contract.</b>
241.	3.4.4 Performance and Scalability Requirements	How will scaling costs be handled?	<b>The scaling costs is to be included as fixed pricing within the recurring hosting line of the cost proposal.</b>
242.	5.2 Evaluation & Attachment D: Cost Form	Are the optional services listed in Attachment D §1.4 evaluated strictly for informational purposes, or do they factor into the Total Cost of Ownership evaluation scoring?	<b>The optional services in Attachment D is to be evaluated for informational purposes and not factored into Total Cost.</b>
243.	3.2.2 Security & Attachment B: IT Terms & Conditions	Can the State clarify how hosting responsibility and associated liability will be allocated between the vendor and the State, particularly with respect to data ownership, breach response, and indemnification obligations?	<b>Hosting and operational responsibility rests with the Vendor under the resulting contract. Data ownership remains with the State at all times. Breach response, indemnification, and limitation of liability are governed by Attachment B (IT Terms and Conditions); Vendors may submit redlines per Question 139. The Vendor is responsible for breach notification to the State within 24 hours of confirmed incident, per Attachment B.</b>

Question #	Solicitation Section	Vendor Question	State's Response
244.	2.3 & 3.3.3 Summary of Problem Statement	The RFP indicates the Student and General Public portals will be unsecured while the Law Enforcement and Admin/Teacher/Support Staff portals will require authentication. Can the State confirm whether authentication is required for all access to those two portals, or only for specific protected sections within them?	<b>Authentication with MFA is required for all access to the Law Enforcement and Admin/Teacher portals (no anonymous content within those portals). See Q226.</b>
245.	3.2.2 Security	Beyond the Vendor Readiness Assessment Report (VRAR) and the listed third-party assessments (FedRAMP, SOC 2 Type 2, ISO 27001, HITRUST), what additional documentation or certification will be required from the vendor regarding hosting and security posture, either at submittal or post-award?	<b>Required at offer submission: completed VRAR, current SOC 2 Type II report (or executive summary if confidential, with full report available under NDA prior to award), evidence of FedRAMP Moderate authorization for the proposed hosting platform, and a current third-party penetration test attestation (full report under NDA acceptable). VPAT is required at offer submission. Detailed network diagrams may use vendor-standard notation and may redact provider-specific operational details, provided all logical components and integration points are shown.</b>
246.	3.4.1 & 3.5 Platform Requirements	Should the proposed solution be architected as standalone applications per portal, or is a single multi-site / multi-tenant configuration acceptable (e.g., WordPress Multisite or Drupal multi-site)?	<b>The four portals shall be implemented as four sections under a single 'Training Portals' tab redirecting to the appropriate authentication or public landing page, on a single multi-site / multi-tenant CMS configuration (e.g., WordPress Multisite or Drupal multi-site). A single CMS back end with separate front ends is not acceptable as proposed in Q134 — a single integrated multi-site solution is required. Audience-specific menus and content listings are required; full distinct branding per portal is not required.</b>

Question #	Solicitation Section	Vendor Question	State's Response
247.	3.1.5 Enterprise Licensing	Given the State's existing Microsoft enterprise agreements, will any Microsoft services, licenses, or Azure tenancy be made available for the awarded vendor to leverage in delivering this solution (e.g., Entra ID, Azure hosting credits, Microsoft 365 services)?	<b>No required cloud provider. Solution must meet FedRAMP Moderate hosting and U.S. data residency requirements. The State has Microsoft enterprise agreements but is not making Azure tenancy, Microsoft 365 services, or Azure hosting credits available to the awarded Vendor for this engagement, except for the limited Entra ID integration described elsewhere.</b>
248.	3.2.2 Security	How will NIST 800-53 Moderate compliance be validated in practice — through documentation review only, a formal audit, inherited controls from the underlying hosting platform, or a combination?	<b>Required at offer submission: completed VRAR, current SOC 2 Type II report (or executive summary if confidential, with full report available under NDA prior to award), evidence of FedRAMP Moderate authorization for the proposed hosting platform, and a current third-party penetration test attestation (full report under NDA acceptable). VPAT is required at offer submission. Detailed network diagrams may use vendor-standard notation and may redact provider-specific operational details, provided all logical components and integration points are shown.</b>
249.	3.2.2 Security	Will the State accept platform-level inheritance for compliance (e.g., FedRAMP-authorized hosting combined with a hardened CMS configuration), or must the CMS application layer itself carry an independent certification?	<b>Hosting must be FedRAMP Moderate authorized at the IaaS/PaaS layer. All data, including backups and disaster recovery copies, shall reside in the continental United States. All Vendor and subcontractor personnel with administrative, support, or production data access must be U.S. persons located in the U.S. GovCloud / Azure Government is not required for this engagement. SOC 2 Type II at the SaaS/application layer combined with FedRAMP Moderate at the underlying platform is acceptable to demonstrate the Moderate baseline, supplemented by the Vendor's completed VRAR.</b>

Question #	Solicitation Section	Vendor Question	State's Response
250.	General	What is the State's target go-live or launch date for the production website? Are there any time-sensitive events (e.g., the RISE Back to School Safety Summit) that should anchor the implementation timeline?	<b>The State has not set a fixed go-live date but the implementation timeline must accommodate the RISE Back to School Safety Summit (annually held in summer / pre-school-year) as a content driver. Vendors may propose phased releases.</b>
251.	3.4.4 Performance and Scalability Requirements	How should auto-scaling and surge-related infrastructure costs be handled in the cost proposal — included as fixed within the recurring hosting line, billed as pass-through based on actual consumption, or itemized separately as an optional service?	<b>The auto-scaling and surge-related infrastructure cost is to be included as fixed pricing within the recurring hosting line of the cost proposal.</b>
252.	3.4.2 Authentication and Access Control Requirements	Given the strict federal and state requirements for public-facing government portals, will the State require the awarded vendor to provide continuous, automated WCAG 2.1 AA and Section 508 accessibility auditing, or is manual, periodic testing deemed sufficient for this contract?	<b>Continuous automated WCAG 2.1 AA / Section 508 accessibility scanning is preferred but not required. Periodic manual testing at minimum quarterly is required, with results reported to CFSS. Critical and serious accessibility findings shall be remediated within 30 days.</b>
253.	3.4.4 Performance and Scalability Requirements	Because the NC Center for Safer Schools acts as a critical public information hub during statewide emergencies, what are the specific Service Level Agreement (SLA) requirements for auto-scaling? Must the vendor provide documented proof of load-balancing capabilities to absorb catastrophic traffic surges (e.g., a 10,000% increase within minutes) without degradation of service?	<b>Auto-scaling shall absorb traffic surges typical of post-event and pre-school-year periods. Specific multipliers are not mandated, but vendor's proposed scaling capacity, load-balancing approach, and performance under surge will be evaluated. Documented evidence of load-balancing capability through a third-party penetration test, performance test report, or platform attestation is required.</b>

Question #	Solicitation Section	Vendor Question	State's Response
254.	3.2.2 Security	Regarding the Content Management System (CMS), will the State require strict adherence to modern security header protocols (such as HSTS, Content-Security-Policy, and X-Frame-Options) upon launch? Furthermore, what is the mandated SLA for patching high-severity CVEs and zero-day vulnerabilities in CMS plugins to prevent malicious site defacement?	<b>Vulnerability scanning shall be performed at minimum monthly and after any significant change. Annual third-party penetration testing is required, with results provided to the State. Critical and High severity vulnerabilities (CVSS 7.0+) shall be remediated within 15 calendar days; Medium within 30 days. Zero-day vulnerabilities affecting the production environment shall be triaged within 24 hours and mitigated/patched within 72 hours, or compensating controls applied. Modern security headers (HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy) are required at launch.</b>
255.	3.3.5 Disaster Recovery and Business Continuity	In the event of a successful ransomware attack or destructive data-wipe by a threat actor, what are the State's mandatory Recovery Time Objective (RTO) and Recovery Point Objective (RPO)? Will the vendor be required to maintain off-site, immutable backups isolated from the primary hosting environment?	<b>Recovery Point Objective (RPO) ≤ 24 hours and Recovery Time Objective (RTO) ≤ 4 hours apply to the full production environment, including all four portals and the CMS-managed embedded content references. Embedded third-party content (Power BI, YouTube, Google Workspace) availability is governed by those providers. Documented manual runbook with tested annual failover is acceptable; fully automatic failover is not required. Off-site, immutable backups isolated from the primary hosting environment are required to defend against ransomware / destructive attack scenarios.</b>
256.	5.2 Evaluation Criteria	To reduce the administrative overhead on State personnel, will the evaluation committee give preference to vendors offering AI-driven or automated backend capabilities (such as automated content tagging, intelligent threat remediation, or AI-assisted accessibility formatting)?	<b>No, AI-driven or automated backend capabilities are not given preference in evaluation. AI use is permitted (Q184) but does not confer scoring advantage.</b>

Question #	Solicitation Section	Vendor Question	State's Response
257.	3.4.3 Content Management Requirements	What is the expected frequency and cadence for content and functional modifications post-launch (e.g., ad-hoc, scheduled, or continuous delivery), and will the State require vendors to support a formal change-management workflow including versioning, rollback, and audit logging for all updates?	<b>All production changes require a formal change management workflow with versioning, rollback capability, and audit logging. NC SBI IT must approve all production changes affecting security configuration, integration endpoints, or authentication. Routine content updates by CFSS authorized users do not require NC SBI IT approval but must be logged.</b>
258.	General	Does the State anticipate adding new pages, sections, or microsities during the contract term, and should vendors architect the solution to scale content and navigation without re-platforming or contract renegotiation?	<b>No major new pages, sections, or microsities are anticipated during the contract term beyond ongoing addition of training dates, training content, images, and content updates. The Vendor shall architect the solution to support content growth without re-platforming.</b>
259.	General	If requested modifications include advanced media production such as video editing, animation, or other non-standard services, will these be managed through a separate purchase order or formal contract amendment, and what approval process will govern such changes?	<b>Contract modifications will be issued either through a separate Purchase Order or a bilateral Amendment.</b>
260.	3.4.2 Authentication and Access Control Requirements	After site launch, the vendor will maintain the platform. What level of administrative access does the State require for its staff, and does the State prefer a role-based access control (RBAC) model that limits full system privileges to reduce operational and security risk?	<b>The Vendor shall implement role-based access control (RBAC) with at minimum the following roles: Administrator, Editor, Author, Viewer, Portal Manager, Approver. Vendor may propose additional granular roles. The State prefers least-privilege; full Administrator privileges shall be limited to the smallest practical set of accounts.</b>
261.	3.4.5 Training Requirements	How does the State prefer training to be delivered for authors and administrators? Would the State value vendors that embed role-based, LMS-style training and contextual guidance directly into the platform rather than relying solely on external documentation or one-time sessions?	<b>Training is for 2-3 internal CFSS users (administrators / content editors). External contributors and Regional School Safety Specialists are not included in the formal training count; they will receive contextual / role-based platform guidance as part of normal operations. Embedded role-based, LMS-style training and contextual guidance within the platform is preferred over external documentation alone.</b>

Question #	Solicitation Section	Vendor Question	State's Response
262.	7.15 Special Terms and Conditions	What level of operational support is required post-launch (business hours vs. 24x7x365), and are defined response and resolution SLAs required for critical, high, and medium severity incidents?	<b>Required post-launch operational support: business hours base support (M–F, 8 AM – 5 PM Eastern) with 24x7 response for Severity 1 incidents; SLAs per Section 7.15. 24x7 base support is an optional priced enhancement.</b>
263.	7.4 Vendor License or Support Agreements	Can the State provide visibility into the current licenses, software subscriptions, and third-party tools used by the incumbent vendor, including user counts and renewal terms, and should the awarded vendor assume responsibility for rationalization or replacement?	<b>Capitol Broadcasting holds the current limited landing page contract through December 2026. No incumbent licenses, subscriptions, or third-party tools transfer to the awarded Vendor; the new Solution is greenfield.</b>
264.	3.3 Enterprise Specifications	What enterprise productivity suite is standardized across the State (e.g., Google Workspace or Microsoft 365 Enterprise), and will the awarded vendor be required to integrate authentication, document workflows, and collaboration features with that platform to align with statewide IT standards?	<b>Microsoft 365 (GCC G5 environment) is the State standardized productivity suite for NC SBI. The awarded Vendor shall integrate authentication for CFSS administrators via Entra ID (Q19, Q235), and shall support embedding of Microsoft-hosted content (Teams recordings, Microsoft Forms) where applicable. Full collaboration / document workflow integration with M365 is not required for this Solution.</b>

2. The correct email address for this Invitation for Bid (IFB) Point of Contact Procurement Specialist is [bhaywood@ncsbi.gov](mailto:bhaywood@ncsbi.gov) and not [bhaywood@nc.gov](mailto:bhaywood@nc.gov).