Selective Service System
Website Modernization FAQ
June 18, 2026

Section 1 – Solicitation Administration & Proposal Submission

Q1.1 – Proposal volume clarification - Section L 2.a states four (4) separately submitted bound Volumes but then enumerates five Volumes (I, II, III, IV, V). Please confirm whether the offeror is expected to submit four bound volumes or five separate volumes. | Section L 2.a, 23

A) We apologize for the confusion. The reference to "four (4) separately electronically submitted bound Volumes" is a typographical error. Offerors shall submit five (5) proposal volumes as identified in the solicitation:

- Volume I – Administrative Proposal
- Volume II – Technical Proposal
- Volume III – Past Performance
- Volume IV – Price Proposal
- Volume V – Contract Documentation

Offerors should prepare and submit all five volumes in accordance with the proposal instructions and content requirements provided in the solicitation. We appreciate your attention to this discrepancy.

Q1.2) Evaluation Factors -Table 1 identifies Volume V as “Factor 5 – Contract Documentation,” but Section 52.212-2 lists only four evaluation factors. Please confirm whether Volume V is evaluated as a separate factor or treated as an administrative/compliance volume only.

A) Yes. Volume V – Contract Documentation corresponds to Evaluation Factor 5. Offerors shall submit Volume V in accordance with the solicitation instructions. Evaluation of Volume V will be conducted in accordance with the evaluation criteria identified in the solicitation.

Q1.3 – Technical and pricing assumptions - Please confirm whether offerors may propose technical assumptions in Volume II and related price assumptions in instructions to Offerors Solicitation. pp. 27 to 29

A) Yes. Offerors may identify reasonable technical assumptions in Volume II and corresponding pricing assumptions in their Price Proposal, provided those assumptions are clearly stated, consistent with the solicitation requirements, and do not take exception to, qualify, or materially alter the Government's requirements. Offerors should clearly document any assumptions used in developing their technical approach, staffing methodology, level of effort, pricing, schedule, or proposed solution. SSS will evaluate proposals based on the requirements of the solicitation and the offeror's demonstrated understanding of those requirements.

Important Note: The Initial Draft Project Plan and Comprehensive Project Timeline shall be submitted with the Technical Proposal. Pages associated with these required submissions are excluded from, and will not be counted toward, the 80-page limitation applicable to Volume II.

Q1.4 Independent Government Cost Estimate (IGCE) - Please provide the Government's Independent Government Cost Estimate (IGCE), budget, total project funding, or anticipated cost range for this requirement.

A) SSS has not established or disclosed a Government estimate, target budget, funding ceiling, anticipated contract value, or expected level of effort for proposal purposes.

Offerors shall independently determine the resources, staffing, labor mix, technologies, hosting services, licenses, integrations, migration activities, security activities, testing, deployment activities, and other elements necessary to satisfy the solicitation requirements and shall base their pricing on their proposed approach.

SSS will evaluate proposals in accordance with the solicitation's stated evaluation criteria. Offerors should clearly document any assumptions that affect pricing, schedule, staffing, or technical performance.

Q1.5 - PPQ subcontractor submission process - Please confirm whether the one required past performance reference must be from the prime offeror only, given the evaluation language stating that past performance where the offeror or subcontractor was not listed as a prime will not be considered relevant. Factor 3 Past Performance, Solicitation pp. 27 to 36

A) Offerors may include information regarding proposed subcontractors and their relevant experience as part of their proposal. Offerors may also identify subcontractor past performance references and include completed Past Performance Questionnaires (PPQs), if available, in Volume III. References are responsible for completing PPQs.

Offerors shall make reasonable efforts to obtain completed PPQs and include them in Volume III of their proposal submission. If a completed PPQ is unavailable by the proposal due date, the offeror may provide the reference's contact information and identify its efforts to obtain the completed PPQ. The Government reserves the right to contact references directly to obtain or verify past performance information. Past performance will be evaluated in accordance with the solicitation's stated evaluation criteria and relevancy requirements. Offerors should clearly identify the role and scope of work to be performed by any proposed subcontractor and explain how the subcontractor's experience supports successful contract performance.

Q1.6 – PPQ submission process -The PPQ instructions state that the reference shall complete and submit the PPQ, while the solicitation states the offeror shall submit the completed PPQ with the proposal package. Please confirm whether the completed PPQ must be submitted directly by the reference, included by the offeror in Volume III, or both. Attachment 2 PPQ, Factor 3, Solicitation pp. 27 to 28.

A) Offerors may include information regarding proposed subcontractors and their relevant experience as part of their proposal. Offerors may also identify subcontractor past performance references and include completed Past Performance Questionnaires (PPQs), if available, in Volume III.

References are responsible for completing PPQs. Offerors shall make reasonable efforts to obtain completed PPQs and include them in Volume III of their proposal submission. If a completed PPQ is unavailable by the proposal due date, the offeror may provide the reference's contact information and identify its efforts to obtain the completed PPQ. SSS reserves the right to contact references directly to obtain or verify past performance information.

Past performance will be evaluated in accordance with the solicitation's stated evaluation criteria and relevancy requirements. Offerors should clearly identify the role and scope of work to be performed by any proposed subcontractor and explain how the subcontractor's experience supports successful contract performance.

Q1.7 Review and approval timelines - What review and approval timelines should offerors assume?

A) SSS will make reasonable efforts to review and provide feedback on deliverables in a timely manner. Specific review timelines have not been established for proposal purposes. Offerors should incorporate realistic review, comment, revision, testing, and approval periods into their proposed schedules. The contract award is expected to be made by **July 15, 2026**, or a date close to this day.

Q1.8 – Post-award meeting date correction - Please confirm whether the post-award meeting due “within 3 business days of award, but no later than September 30, 2026” should be interpreted as within 3 business days of award. | PWS 7.1 | Attachment 1, p. 16

A) The correct date for the post award meeting should read July 20, 2026, three business days after the awarding of the contract on July 15, 2026.

Q1.9 – Substantial Completion Milestones (Website delivery) - Please clarify what activities are included within the September 25, 2026 substantial-completion milestone.

A) For purposes of this solicitation, the September 25, 2026 substantial-completion milestone represents completion of the implementation activities necessary to support SSS's planned deployment objectives for the modernized website solution.

By the substantial-completion date, the Contractor shall have completed all required discovery, design, development, configuration, migration, integration, testing, training, documentation, deployment preparation, and other implementation activities necessary to deliver a production-ready solution to SSS. The solution should be fully configured, tested, and prepared for operational cutover, subject to final Government acceptance and any remaining authorization activities.

SSS may accept a solution that is "cutover ready" by September 25, 2026, provided all required implementation activities have been completed, required testing has been successfully performed, critical defects have been resolved, deployment readiness has been demonstrated, and all required authorization activities are progressing in accordance with the approved security and authorization process.

The September 25, 2026 milestone does not alter the requirements applicable to operations and sustainment activities, transition activities, option periods, or other post-implementation requirements identified elsewhere in the solicitation.

Offerors shall propose an approach that satisfies the solicitation requirements, milestones, and schedule and should clearly identify any assumptions regarding Government reviews, approvals, authorization activities, dependencies, or deployment sequencing.

Q1.10 – Proposal file formats - Section 2(b) states that proposal files shall be submitted in Microsoft Word or Excel formats and that PDF files are permitted for executed documents such as the Cover Letter. Please confirm whether Technical, Past Performance, Administrative, and other proposal volumes may be submitted in PDF format for readability, formatting control, and electronic review. | Section L, Proposal Structure and Details

A) Offerors shall follow the file format instructions identified in the solicitation.

SSS acknowledges that clarification may be required regarding acceptable proposal file formats and submission requirements. SSS will review the solicitation language and provide clarification through a solicitation amendment, if necessary.

Until further clarification is issued, offerors should prepare proposal submissions in accordance with the instructions contained in the solicitation.

Q1.11 – Proposal compliance verification - Volume II requires offerors to provide verification of compliance with the security requirements identified in PWS Section 2.4. Please clarify the level and format of detail expected for this verification (e.g., narrative confirmation, attestations, certifications, supporting documentation, or evidence of existing compliant capabilities). | Volume II; PWS 2.4

A) Offerors should provide sufficient information to demonstrate compliance with the security requirements identified in PWS Section 2.4.

Verification may include narrative descriptions, attestations, existing authorizations or certifications, supporting documentation, architectural descriptions, security controls, compliance approaches, or other evidence the offeror determines appropriate to substantiate compliance with the solicitation requirements.

SSS will evaluate submissions in accordance with the solicitation requirements and evaluation criteria.

Section 2 – Evaluation, Past Performance & Staffing

Q2.1 – PPQ process - Section 52.212-1 Addendum, Volume III, states: "the offeror shall also send the Past Performance Questionnaire at Attachment 2 to the one designated reference and have them complete it and the offeror shall submit the completed Attachment 2 questionnaire to the Government with their proposal package by the submittal closing date." However, Attachment 2 itself instructs the reference to "complete this Questionnaire and e-mail to Contracting Officer, G. Hendricksen" and "Contract Specialist, Shimere Cooper" directly. Please clarify the required submission method: (a) Should the completed PPQ be emailed directly by the reference to the Contracting Officer and Contract Specialist? (b) Should the Offeror collect the completed PPQ from the reference and include it in the Offeror's proposal package? (c) Both? Section 52.212-1 Addendum, Volume III (Pages 27-28); Attachment 2, 27-28; Attachment 2, Page 1

A) Offerors may include information regarding proposed subcontractors and their relevant experience as part of their proposal. Offerors may also identify subcontractor past

performance references and include completed Past Performance Questionnaires (PPQs), if available, in Volume III. References are responsible for completing PPQs.

Offerors shall make reasonable efforts to obtain completed PPQs and include them in Volume III of their proposal submission. If a completed PPQ is unavailable by the proposal due date, the offeror may provide the reference's contact information and identify its efforts to obtain the completed PPQ. The Government reserves the right to contact references directly to obtain or verify past performance information.

Past performance will be evaluated in accordance with the solicitation's stated evaluation criteria and relevancy requirements. Offerors should clearly identify the role and scope of work to be performed by any proposed subcontractor and explain how the subcontractor's experience supports successful contract performance.

Q2.2 – PPQ evaluation treatment - If the Offeror's designated reference is unable to submit the completed Attachment 2 (PPQ) by the proposal due date of June 30, 2026, despite the Offeror's diligent efforts, will the Government accept a late-submitted PPQ from the reference, or will the Offeror's past performance be rated as "Neutral" per the evaluation criteria in Table 5? Section 52.212-2 Addendum, Factor 3, Table 5 (Performance Confidence Assessments), 36

A) Offerors are responsible for ensuring that past performance information is submitted in accordance with the solicitation instructions and by the required deadline.

SSS will evaluate past performance using the information submitted with the proposal, information obtained from references, CPARS reports, and any other sources identified in the solicitation. SSS cannot guarantee that past performance information received after the proposal due date will be considered during the evaluation process. If sufficient past performance information is not available for evaluation, SSS will assign a past performance confidence assessment in accordance with the solicitation's stated evaluation criteria, including the Neutral Confidence rating, when applicable.

Q2.3 – Subcontractor experience - The instructions for Volume III-Factor 3-Past Performance & Capability Statement state that “The offeror shall provide one (1) Past Performance reference using the Past Performance Questionnaire at Attachment 2. The reference shall be from relevant and recent contracts, on-going contracts, subcontracts and/or task/delivery orders accomplished within the past three (3) years.” Can the Government confirm that the Offeror (either prime or subcontractor on this SSS solicitation) can submit a past performance for work that they have performed as a subcontractor? Addendum - Instructions 2.f, 27-28

A) Offerors may submit past performance references for work performed as a subcontractor, provided the reference is relevant in size, scope, and complexity to the requirements of this solicitation. Past performance information from proposed

subcontractors or teaming partners may be considered when the offeror demonstrates how that experience is relevant to the proposed solution and how the proposed subcontractor or teaming partner will meaningfully contribute to contract performance. SSS will evaluate past performance in accordance with the solicitation's evaluation criteria. The Government will review any apparent inconsistencies between the submission instructions and evaluation criteria and provide clarification through a solicitation amendment, if necessary.

Q2.4 – Labor category structure - The solicitation requires price backup detail by labor category and labor hours. Does the Government have a preferred labor category structure, or should offerors propose their own role-based labor categories? Price Proposal, Solicitation pp. 28 to 29

A) The solicitation requires offerors to provide pricing support at the labor category and labor-hour level; however, the solicitation does not appear to prescribe a specific Government labor category structure or standardized labor category matrix.

Accordingly, offerors may reasonably interpret the solicitation as allowing them to propose their own labor category structure, provided the proposed labor categories clearly align with the technical approach, staffing plan, labor mix, and performance requirements, and provide sufficient detail for the Government to evaluate price realism, reasonableness, and completeness.

Q2.5 – Commercial references - Please confirm whether the single required past performance reference may be from Federal, State, Local/Municipal, or Commercial customers, provided it is recent and relevant? Volume III / Factor 3 – Past Performance; Evaluation – Past Performance, pp. 27–28 and p. 35

A) Offerors should submit recent and relevant past performance references in accordance with the solicitation instructions. References may be from Government or commercial customers, provided they demonstrate experience relevant to the requirements of the solicitation. The Government will evaluate all references in accordance with the stated evaluation criteria.

Q2.6 – Prime/subcontractor relevancy - Please confirm whether the one required past performance reference must be from the prime offeror only, given the evaluation language stating that past performance where the offeror or subcontractor was not listed as a prime will not be considered relevant. Factor 3 Past Performance, Solicitation pp. 27 to 36

A) Offerors may include information regarding proposed subcontractors and their relevant experience as part of their proposal. Offerors may also identify subcontractor past performance references and include completed Past Performance Questionnaires (PPQs), if available, in Volume III.

References are responsible for completing PPQs. Offerors shall make reasonable efforts to obtain completed PPQs and include them in Volume III of their proposal submission. If a completed PPQ is unavailable by the proposal due date, the offeror may provide the reference's contact information and identify its efforts to obtain the completed PPQ. The Government reserves the right to contact references directly to obtain or verify past performance information.

Past performance will be evaluated in accordance with the solicitation's stated evaluation criteria and relevancy requirements. Offerors should clearly identify the role and scope of work to be performed by any proposed subcontractor and explain how the subcontractor's experience supports successful contract performance.

Q2.7 – Commercial References - May offerors submit commercial-sector references, or are references limited to Federal Government contracts?

A) Offerors may submit references from Federal, state, local, tribal, commercial, or other organizations, provided the work is relevant in size, scope, complexity, and technical characteristics to the requirements of this solicitation.

SSS will evaluate past performance based on the degree to which the referenced effort demonstrates experience performing work similar to the requirements of this solicitation. The customer type is less important than the relevance of the work performed.

Q2.8 – Past Performance References - Must the submitted past performance reference involve Federal website modernization or Federal digital services projects?

A) No. References are not required to involve Federal website modernization projects specifically. Offerors may submit references that demonstrate relevant experience performing similar website modernization, content management, cloud hosting, application integration, cybersecurity, digital experience, conversational AI, or related services.

SSS will evaluate past performance in accordance with the solicitation's stated evaluation criteria, including relevance in size, scope, and complexity.

Q2.9 – Reliance on subcontractors to demonstrate capabilities - May the prime contractor rely on the experience of proposed subcontractors to demonstrate capability and past performance?

A) Yes. Offerors may reference the experience and past performance of proposed subcontractors when such subcontractors are expected to perform meaningful portions of the contract effort. Offerors should clearly identify the proposed subcontractor, the work the subcontractor is expected to perform, and the relevance of the referenced experience to the requirements of this solicitation.

Q2.10 – Small business workshare - Does the prime small business offeror's workshare count toward small business participation?

A) For this 100 percent Small Business Set-Aside, the prime contractor's proposed performance of the contract may be included as part of the overall small business participation approach. Offerors shall comply with applicable limitations on subcontracting and submit the documentation required by the solicitation. A separate subcontracting plan is not required unless specifically identified elsewhere in the solicitation.

Q2.11 – Total estimate level of effort -- Section 52.212-2, Factor 4, refers to the "total estimated level of effort cited in the PWS." Please identify where the Government-provided estimated level of effort is located.

A) SSS is not aware of a Government-provided estimated level of effort identified in the solicitation. Offerors shall independently determine the staffing, labor mix, level of effort, and resources necessary to successfully perform the requirements of the solicitation and should clearly document any associated assumptions.

Q2.12 – Prescribed labor categories - Will SSS provide prescribed labor categories, labor hours, staffing levels, or labor mix requirements?

A) SSS has not established prescribed labor categories, staffing levels, labor hours, or labor mix requirements for proposal purposes. Offerors shall propose the personnel, labor categories, staffing approach, and level of effort they determine necessary to successfully perform the solicitation requirements and should clearly identify any assumptions affecting staffing, schedule, or performance.

Q2.13 – Mapping personnel - Are offerors required to map personnel to specific Government labor categories?

A) No specific Government labor category structure has been established for proposal purposes. Offerors may utilize their own labor category structure, provided proposed personnel qualifications, responsibilities, and experience clearly demonstrate the capability to successfully perform the solicitation requirements.

Section 3 – Pricing, CLINs & Contract Structure

Q3.1 – Operations Testing Platform pricing - Please confirm whether the Operations Testing Platform optional CLIN should be priced for the base period, option years, or both, and whether it should be included in the initial technical schedule. PWS Part 6, CLIN 5001, Solicitation p. 8 and Attachment 1, pp. 14 to 15

A) CLIN 5001 is identified as an optional CLIN. Offerors shall provide pricing for the Operations Testing Platform in accordance with the solicitation's pricing instructions and their proposed technical approach. SSS has not established specific quantities, periods of use, labor-hour estimates, or exercise timing for this optional CLIN. Offerors should develop reasonable assumptions and provide sufficient supporting detail to substantiate their proposed approach and pricing.

Offerors may include activities associated with the optional Operations Testing Platform in their proposed schedule to the extent necessary to demonstrate readiness to perform the work if the CLIN is exercised. Actual implementation, timing, scope, and period of performance for CLIN 5001, if exercised, will be determined by the Government in accordance with the contract.

For evaluation purposes, the Government will assess the Offeror's technical approach for performing the requirements associated with CLIN 5001. Although Offerors are required to submit pricing for this optional CLIN, the proposed price for CLIN 5001 will not be separately evaluated and will not be included in the Government's calculation of the total evaluated price for award purposes.

Q3.2 – Website enhancement and features - Regarding the CLIN structure: please confirm that Option Year CLINs cover continuing hosting, operations and sustainment, security monitoring, and chatbot optimization (PWS 5.2) at steady-state, and clarify how the Government intends CLIN 0004 (Enhancement & Feature Development) to be priced — e.g., as a Government-defined level of effort, NTE pool, or other structure.

A) SSS has revised the solicitation through amendment to designate the requirements identified in PWS Part 5, including PWS 5.2, as required contract requirements to be addressed within the applicable CLIN structure and pricing schedule.

Offerors shall propose the labor mix, level of effort, technical approach, and pricing they determine necessary to successfully perform the required contract services and deliverables identified in the solicitation. SSS is not prescribing a specific level of effort, not-to-exceed value, staffing level, labor mix, or pricing methodology beyond what is identified in the solicitation and associated pricing schedule. Offerors shall complete the pricing sheet in accordance with the solicitation instructions.

The Government will evaluate the Offeror's proposed technical approach for satisfying the requirements associated with this CLIN in accordance with the solicitation's technical evaluation criteria. Proposed pricing will be evaluated as part of the overall price evaluation in accordance with the solicitation.

Q3.3 – Base Pricing - The 52.212-2 Addendum (Factor 4, Price Proposal Evaluation) states that any proposal "not within the total estimated level of effort cited in the PWS" shall include an explanation; however, the PWS does not cite an estimated level of effort, labor hours, or budget range. Please provide the estimated level of effort or clarify how price realism will be assessed in its absence., Section V, 52.212-2 Addendum, Factor 4, 36.

A) Offerors shall propose pricing based on their own technical approach and the requirements set forth in the solicitation. SSS is not prescribing a specific level of effort, not-to-exceed value, staffing level, or pricing structure beyond what is identified in the solicitation and associated pricing schedule. Offerors shall propose the labor mix, level of effort, and pricing they determine necessary to successfully perform the requirements. Offerors should clearly document any assumptions that materially affect pricing, staffing, schedule, or performance.

Q3.4 – CLIN Pricing - Amendment 0002 states that SSS can accept a "cutover ready" solution to support the September 25, 2026 deadline. Please clarify whether the September 25, 2026 substantial-completion date applies only to implementation activities or whether it also includes operations and sustainment activities under CLIN 0003, transition activities, and optional CLINs.

A) The September 25, 2026 substantial-completion milestone applies to the implementation, modernization, migration, integration, testing, deployment readiness, training, documentation, and related activities necessary to achieve the required project objectives. Operations and sustainment activities, transition activities, option periods, and optional CLINs, if exercised, will be performed in accordance with their respective contract periods, performance requirements, and contract terms.

SSS may accept a solution that is "cutover ready" by the required completion date, provided all required authorization activities are progressing in accordance with the approved security and authorization process.

Q3.5 – AI Chatbot - If the Government's existing conversational AI platform is leveraged, who is responsible for licensing, subscriptions, usage-based charges, and recurring costs during the base period and option years?

A) If an offeror proposes to leverage a Government-furnished conversational AI capability, SSS will provide additional information regarding ownership, licensing, subscription arrangements, and associated responsibilities following award, as appropriate.

Offerors should clearly identify any assumptions regarding licensing, subscription costs, consumption-based charges, and ongoing operational support within their proposals and pricing.

Q3.6 – AI Chatbot Messaging - Will SSS provide written authorization to use SSS-generated FAQs, user guides, and public-facing documentation to build the chatbot?

A) SSS may provide approved public-facing content, including FAQs, user guides, website content, policy information, and other Agency-approved materials, for use in configuring and supporting the conversational AI solution. The chatbot knowledge base will be derived from Government-approved content sources. Any use of Government content shall comply with the solicitation's AI governance, privacy, security, and data protection requirements. Additional details regarding approved content sources, formats, and governance processes will be provided following award, as appropriate.

Q3.7 – Transition Out Phase - PWS Part 5.5 requires migration from the Contractor-hosted cloud environment to a Government-designated environment during transition-out. Please clarify whether the production environment is expected to remain contractor-hosted during the base period and option years.

A) The solicitation contemplates a contractor-provided hosting environment during contract performance. The transition-out requirement is intended to ensure the orderly transfer of website assets, data, configurations, documentation, application components, and related materials to a Government-designated environment or successor contractor at the conclusion of performance.

SSS has not established a requirement for migration to a Government-owned environment during the base period or option periods unless otherwise directed.

Q3.8 – Transition-out pricing - Please confirm whether transition-out support under CLIN 6001 should be priced as an optional CLIN, included in the base price, or priced only if separately exercised. CLIN 6001, PWS 5.5, Solicitation p. 9 and Attachment 1, pp. 13 to 14

A) CLIN 6001 is identified as a separate CLIN for transition-out support. Offerors should provide pricing for CLIN 6001 in accordance with the solicitation's pricing instructions and should not include transition-out support costs within the base contract pricing unless otherwise reflected in their proposed pricing structure.

SSS has not established a specific quantity, labor-hour estimate, or exercise date for transition-out activities. Offerors should develop reasonable assumptions and provide sufficient supporting detail to allow evaluation of the proposed pricing. Transition-out support will be performed only if required by SSS and in accordance with the terms of the contract. Offerors should clearly identify any assumptions used in developing their proposed pricing for CLIN 6001.

Q3.9 – Small Business Participation and Contract Structure - The solicitation is a 100% Small Business Set-Aside and Volume V requires contract documentation related to small business participation. Please confirm whether the prime small business offeror's own proposed workshare counts toward the required small business participation commitment and whether a separate subcontracting plan is required.

A) For this 100 percent Small Business Set-Aside, the prime contractor's proposed performance of the contract may be included as part of the overall small business participation approach. Offerors shall comply with the applicable limitations on subcontracting and submit the documentation required by the solicitation. A separate subcontracting plan is not required unless specifically identified elsewhere in the solicitation.

Q3.10 – Scope of Substantial Completion vs. Contract Periods - Amendment 0002 states that SSS can accept "cutover ready" for the ATO timeline in order to meet deadlines. Please clarify whether the September 25, 2026 substantial-completion date applies to initial modernization/development, testing, UAT, and cutover readiness only, or whether it also applies to operations and sustainment activities under CLIN 0003, transition-out activities, and optional/future CLINs.

A) The September 25, 2026, substantial-completion milestone applies to the implementation, modernization, testing, migration, integration, deployment readiness, and related activities necessary to achieve the required project objectives. Operations and sustainment activities, transition activities, option periods, and optional CLINs, if exercised, will be performed in accordance with their respective contract periods and requirements.

SSS may accept a solution that is "cutover ready" by the required completion date, provided all required authorization activities are progressing in accordance with the approved security and authorization process.

Q3.11 – Post-Award Meeting and Contract Kickoff Structure - Amendment 0002 confirms the anticipated award date is July 15, 2026. PWS 7.1 schedules the Post-Award Meeting "within 3 business days of award," but also states "no later than September 30, 2026." Please confirm whether the September 30, 2026 date is intentional or should be corrected.

A) The Post-Award Meeting shall occur within three (3) business days of contract award. Based on the anticipated award date of July 15, 2026, the intended meeting date is July 20, 2026. The September 30, 2026 date appears inconsistent with the solicitation schedule and should be considered a clerical error pending formal correction.

Q3.12 – Contract Deliverable Structure - Does substantial completion require a fully operational production deployment by September 25, 2026?

A) The September 25, 2026 milestone is intended to ensure the modernized website, integrations, migration activities, testing, and deployment preparations are completed and ready to support SSS deployment objectives. SSS may accept a solution that is cutover-ready by the required completion date, provided testing, deployment readiness, and authorization activities are substantially complete and progressing in accordance with the approved implementation and authorization process.

Q3.13 – Contract Performance Schedule - Please clarify the relationship between the September 25, 2026 substantial-completion date and the subsequent operations and sustainment period. Does contract performance end upon delivery of the modernized website, or does performance continue under a separate operations and sustainment period beginning September 26, 2026?

A) The September 25, 2026 substantial-completion milestone applies to the implementation phase of the effort, including modernization, design, development, migration, integration, testing, security documentation, deployment readiness, and related implementation activities necessary to achieve the required project objectives.

Contract performance does not end upon substantial completion of the website. Following substantial completion, operations and sustainment activities shall continue in accordance with the applicable contract line items (CLINs), contract periods of performance, and solicitation requirements. For planning purposes, offerors should assume that implementation activities culminate with substantial completion on September 25, 2026, and that the subsequent operations and sustainment period begins immediately thereafter, consistent with the contract structure and periods of performance identified in the solicitation.

Transition-out activities, option periods, and any optional CLINs, if exercised, shall be performed in accordance with their respective contract requirements and performance periods.

Section 4 – Schedule, Reviews & Deliverables

Q4.1 – Substantial completion - The solicitation states all work must be “substantially completed” by September 25, 2026. Please define “substantial completion” (e.g., production launch, Government acceptance, completion of testing/UAT, completion of content migration, ATO status).

A) For purposes of this solicitation, substantial completion refers to the successful production deployment of the modernized website by September 25, 2026. Activities required to achieve full operational capability, including final documentation, training, transition, chatbot implementation, security authorization activities, and other post-deployment requirements, may continue in accordance with the approved project schedule and contract requirements.

Q4.2 – Deployment readiness - Please clarify the acceptance criteria for "substantially completed" by September 25, 2026, including whether this means production deployment, UAT completion, security approval, content migration completion, ATO approval, training completion, and closeout. Technical Capability and Project Schedule, PWS 7.1, Solicitation p. 25 and Attachment 1, pp. 16 to 17

A) For proposal purposes, "substantially completed" means that the modernized website solution is functionally complete and ready for transition to production operations by September 25, 2026. At a minimum, SSS expects core development, testing, content migration, training, and user acceptance activities necessary to support deployment readiness to be substantially complete.

The solicitation does not establish detailed acceptance criteria or mandatory completion milestones for individual activities such as production deployment, final content migration, training completion, security authorization issuance, contract closeout, or other post-implementation activities. SSS will work collaboratively with the successful contractor after award to refine implementation milestones, deployment readiness criteria, testing requirements, authorization activities, and transition planning.

Q4.3 – Government review timelines - What are SSS's expected timelines for design approvals, security reviews, AI conversation approvals, and UAT sign-off? Can SSS support expedited review cycles (24–72 hours) given the compressed schedule? Government Review Process; Timeline and Schedule Feasibility

A) SSS will make reasonable efforts to review and provide feedback on discovery deliverables, design specifications, security documentation, AI governance submissions, UAT results, production readiness materials, and other required deliverables in a timely manner.

SSS has not established specific review, comment, approval, or acceptance turnaround times for proposal purposes. Offerors should propose a realistic project schedule that includes adequate time for SSS reviews, comments, revisions, testing activities, stakeholder coordination, security authorization activities, and approval processes.

Offerors are responsible for identifying and managing schedule dependencies, assumptions, risks, and Government review activities within their proposed project plans.

Q4.4 – Award/kickoff correction - Please confirm whether the post-award meeting due "within 3 business days of award, but no later than September 30, 2026" should be interpreted as within 3 business days of award. | PWS 7.1 | Attachment 1, p. 16

A) The correct date for the post award meeting should read July 20, 2026, three business days after the awarding of the contract on July 15, 2026.

Section 5 – Security, RMF & Authorization

Q5.1 – Security framework - Does SSS have an existing Authority to Operate (ATO) for the current website that the contractor will inherit and update, or will the contractor be responsible for building a new ATO from scratch under this contract?

A) The modernized website and supporting solution will require authorization as a new system. Offerors should assume responsibility for supporting the security, compliance, documentation, testing, and authorization activities necessary to achieve an Authority to Operate (ATO) for the contractor-provided solution in accordance with applicable Federal and agency requirements.

To support the required implementation timeline, the Government may accept a solution that is "cutover ready" while final authorization activities are being completed, provided all required security, testing, compliance, and deployment readiness criteria have been satisfied and the Government determines that deployment can proceed in accordance with applicable risk management and authorization processes.

The solicitation establishes the Government's security and compliance objectives but does not prescribe all detailed ATO documentation, control implementation, assessment procedures, or authorization timelines for proposal purposes.

SSS will work collaboratively with the successful contractor after award to refine authorization requirements, provide applicable domain and system information, coordinate security activities, and support the completion of required ATO-related activities.

Q5.2 – Authorization responsibilities - Regarding Authority to Operate (ATO) requirements: (a) Does the current SSS website have an active ATO? Will the new website solution inherit an existing system security boundary, or will a new ATO package be required from scratch? (b) Will the Selective Service System designate an Information System Security Officer (ISSO) and Authorizing Official (AO) for this effort? Is the contractor expected to provide ISSO support? (c) Is the contractor expected to achieve a full ATO within the September 25, 2026, deadline, or will an Interim Authority to Operate (IATO) or

Authority to Test (ATT) be acceptable at launch? | PWS Part 2.4 / Section V, Factor 2, Items 9-10 Solicitation pp. 26-27

A) The modernized website and supporting solution will require authorization as a new system. Offerors should assume responsibility for supporting the security, compliance, documentation, testing, vulnerability management, assessment, and authorization activities necessary to achieve an Authority to Operate (ATO) for the contractor-provided solution in accordance with applicable Federal and agency requirements.

The solution shall be designed and implemented consistent with applicable Federal cybersecurity requirements, including Risk Management Framework (RMF) processes, FIPS 199 Moderate impact-level requirements, NIST security controls, vulnerability management requirements, and other applicable agency security standards.

To support the required implementation timeline, SSS may accept a solution that is cutover ready while final authorization activities are being completed, provided all required security, testing, compliance, remediation, and deployment-readiness criteria have been satisfied and SSS determines deployment can proceed in accordance with applicable risk management and authorization processes.

Following award, SSS will provide available Government-furnished security information, inherited control information, authorization artifacts, templates, architecture information, interface documentation, and other materials necessary to support contract performance, as appropriate. Because the modernized website and supporting solution will be authorized as a new system, offerors should not assume that all requested security artifacts currently exist in a form directly reusable for the new authorization effort.

The solicitation establishes SSS's security and compliance objectives but does not prescribe all detailed authorization boundary definitions, control implementation approaches, assessment procedures, vulnerability remediation processes, documentation requirements, or authorization timelines for proposal purposes. SSS will work collaboratively with the successful Contractor following award to refine authorization requirements, coordinate security activities, identify inherited controls a

Q5.3 – CMS authorization boundary - For a custom-developed CMS that is not a separately marketed commercial product, the CMS would be documented and authorized as part of the overall system ATO at FIPS 199 Moderate under the NIST Risk Management Framework, rather than holding an independent FedRAMP authorization. Please confirm that this approach is acceptable for meeting the security compliance requirements at PWS 2.4, provided the CMS is fully covered by the system's SSP, control implementation evidence, and ATO boundary documentation., Attachment 1, PWS 2.4 (Security Compliance and Access and Authentication), 4-5 (Attachment 1, Pages 4-5)

A) SSS has not prescribed a specific authorization approach for individual application components, content management systems, or software modules within the proposed solution.

Offerors may propose solutions that satisfy the solicitation's security, authorization, hosting, content management, and compliance requirements. Offerors should clearly describe their proposed architecture, authorization boundary, security control implementation approach, and how all components of the proposed solution will be addressed within the applicable authorization package, system security documentation, and authorization process.

For proposal purposes, SSS does not require a separate FedRAMP authorization, independent Authority to Operate (ATO), or standalone authorization package for individual CMS components that are part of the overall proposed solution. The Contractor shall be responsible for demonstrating how the proposed solution satisfies applicable security and authorization requirements.

Proposed solutions will be evaluated in accordance with the solicitation requirements and evaluation criteria.

Q5.4 – SSS cybersecurity Support - Please confirm whether SSS will provide existing security artifacts, including current SSP, security boundary diagrams, inherited/shared control matrix, POA&M, FedRAMP inheritance expectations, prior assessment results, penetration test reports, and continuous monitoring requirements. | Attachment 1 PWS 2.4 and 7.2 Attachment 1 pp. 4-6, 17-19 / PDF pp. 41-43, 54-56

A) Following award, SSS will provide available Government-furnished security information, documentation, inherited control information, security requirements, architecture information, assessment documentation, authorization artifacts, templates, and other materials necessary to support contract performance, as appropriate.

Such information may include, if available and applicable, security documentation, system architecture information, inherited/shared control information, authorization artifacts, assessment results, continuous monitoring requirements, templates, and other relevant materials.

Because the modernized website and supporting solution will be authorized as a new system, offerors should not assume that all requested artifacts currently exist in a form directly reusable for the new authorization effort.

Q5.5 – Cybersecurity monitoring - Please identify any SSS-required cybersecurity tools, SIEM destinations, log formats, monitoring integrations, vulnerability scanners, ticketing systems, or reporting templates that the Contractor must use or integrate with. | Attachment 1 PWS 2.1, 2.4, 2.8, and 5.3 Attachment 1 pp. 2-7, 12 / PDF pp. 39-44, 49

A) Following award, SSS will provide available information regarding required security integrations, monitoring requirements, reporting requirements, interface specifications, Government-furnished services, and other technical requirements necessary to support contract performance, as appropriate.

At this time, SSS has not prescribed specific cybersecurity products, SIEM platforms, vulnerability scanners, ticketing systems, log formats, monitoring tools, or reporting templates beyond the requirements identified in the solicitation. Offerors may propose solutions that satisfy the solicitation's security, monitoring, logging, reporting, compliance, and operational requirements.

Where integration with Government-managed security services, monitoring capabilities, reporting processes, or other enterprise services is required, detailed technical requirements and interface information will be provided to the successful contractor following award, as appropriate.

Q5.6 – Contractor-managed cloud environment - If the solution is hosted in a Contractor-managed cloud environment, please clarify whether SSS requires direct administrative access, read-only audit access, security tool access, billing visibility, source code repository access, and cloud configuration visibility. Attachment 1 PWS 2.1, 2.4, and 5.5 | Attachment 1 pp. 2-6, 13-14 / PDF pp. 39-43, 50-51

A) SSS requires sufficient access, visibility, reporting, and oversight capabilities necessary to support contract administration, security oversight, audit activities, incident response coordination, compliance verification, and operational requirements.

The Solicitation does not currently prescribe requirements regarding administrative privileges, cloud account ownership, source code repository access, billing visibility, security tool access, audit access levels, or cloud configuration access. The specific access, reporting, monitoring, and visibility requirements for the contractor-managed environment will be coordinated with the successful contractor following award.

Offers should describe their proposal approach for providing appropriate Government visibility into system operations, security posture, compliance activities, reporting, and performance while maintaining effective management of the contractor-provided hosting environment.

Q5.7 – Disaster Recovery Capabilities - Please clarify whether the Contractor must provide disaster recovery capabilities for only the public website and CMS or also for chatbot, staging, analytics, logs, document storage, integrations, and optional testing platform components. | Attachment 1 PWS 2.1, Cloud Infrastructure and Hosting; PWS 8.1, Attachment 1 pp. 2-3, 22-26 / PDF pp. 39-40, 59-63

A) The Contractor's disaster recovery and continuity capabilities should address the contractor-provided solution and any contractor-managed components necessary to satisfy the solicitation's availability, security, operational, and recovery requirements.

This may include, as applicable, the public website, content management system (CMS), conversational AI capability, contractor-managed storage, logging, monitoring, analytics, integration services, and other contractor-operated components supporting the modernized website solution.

SSS has not established component-specific disaster recovery requirements for individual solution elements beyond the requirements identified in the solicitation. Offerors should describe their proposed disaster recovery, continuity of operations, backup, recovery, and resilience approach for the components included within their proposed solution.

Q5.8 Access Authorization - Please confirm the authoritative identity provider for CMS/backend portal access and whether SSS requires Azure AD/Entra ID, Login.gov, PIV/CAC, or another approved authentication mechanism for each user population. | Attachment 1 PWS 2.4, Security Compliance and Access and Authentication | Attachment 1 pp. 4-6 / PDF pp. 41-43

A) For contractor personnel and authorized SSS users requiring access to the CMS, administrative functions, management interfaces, and other privileged capabilities, SSS currently anticipates utilizing Microsoft Entra ID (Azure Active Directory) and other approved Government identity services, as applicable.

Authentication, identity proofing, registration updates, document uploads, and related transaction processing for public users are provided through existing or future Selective Service System mission systems and are not required to be implemented as part of the contractor-provided website.

Detailed identity management, role-based access control, privileged access, MFA requirements, integration specifications, and user population requirements will be coordinated with the successful Contractor following award. Offerors should propose solutions consistent with the solicitation requirements and applicable Federal identity, authentication, and security standards.

Q5.9 – Multi-Factor Authentication - Please clarify whether MFA must be enforced through SSS's identity provider, the CMS, the cloud platform, or all applicable layers, and whether any break-glass, service account, or privileged access procedures are required. | Attachment 1 PWS 2.4; PWS 8.1 Security Compliance, Attachment 1 pp. 4-6, 22-26 / PDF pp. 41-43, 59-63

A) Multi-factor authentication (MFA) shall be implemented consistent with applicable Federal security requirements and the authentication architecture of the proposed solution. MFA is expected to be enforced for privileged, administrative, management, and other authorized user access, as applicable.

For contractor personnel and authorized SSS users, MFA requirements may be implemented through Microsoft Entra ID, other approved Government identity services, the CMS, the cloud platform, or a combination thereof, depending on the final solution architecture and access model.

Offerors should describe their proposed approach to MFA enforcement, privileged access management, service account management, emergency access ("break-glass") procedures, and related security controls. Detailed identity, access management, and privileged access requirements will be coordinated with the successful Contractor following award and shall comply with applicable Federal security standards and agency requirements.
There may not be a requirement for contractors to access SSS IT infrastructure and back-end systems. But a plan should be devised for contingency purposes.

Q5.10 – Plan to Monitor User Access - Please identify audit logging requirements for CMS/backend users, including events to log, retention period, export format, SIEM destination, log review frequency, and whether SSS requires immutable or tamper-evident logging. | Attachment 1 PWS 2.4, 2.6, and 2.8 Attachment 1 pp. 4-7 / PDF pp. 41-44

A) This project likely will not require back-end access to SSS IT infrastructure and information systems. However, offerors shall implement audit logging capabilities consistent with applicable Federal cybersecurity requirements, including OMB M-21-31, applicable NIST guidance, CISA recommendations, agency security requirements, and the security architecture of the proposed solution.

At a minimum, audit logging should support the monitoring and investigation of authentication events, privileged user activities, administrative actions, configuration changes, content management activities, security-relevant events, and other activities necessary to support security, compliance, operational oversight, and incident response.

SSS has not established specific requirements regarding event-level logging, retention periods, export formats, SIEM platforms, log review frequencies, immutable logging technologies, or tamper-evident logging mechanisms for proposal purposes. Offerors should describe their proposed approach to audit logging, log retention, monitoring, reporting, integrity protection, and security event management consistent with applicable Federal requirements and the proposed solution architecture.

Detailed logging, monitoring, reporting, and integration requirements, including any Government-managed security services or monitoring capabilities, will be coordinated with the successful Contractor following award, as appropriate.

Q5.11 – AI Chatbot Deployment - Please confirm whether the Government requires a FedRAMP-authorized chatbot platform specifically, or whether a chatbot deployed within a FedRAMP-authorized cloud environment and formally approved by SSS is acceptable.| Attachment 1 PWS 3.2; 52.212-1 Addendum, Factor 2, Submittal Verification, Attachment 1, p. 9 / PDF p. 46; SF1449

A) Offerors shall propose a conversational AI solution that satisfies the solicitation's security, privacy, hosting, compliance, and operational requirements.

A chatbot solution deployed within a FedRAMP-authorized cloud environment is preferable, provided the overall solution architecture satisfies applicable Federal and agency security requirements and receives the necessary SSS approvals. However, SSS does not require a separate, standalone FedRAMP authorization for the chatbot component if the proposed solution is implemented within an approved authorization boundary and complies with applicable security requirements.

Offerors should clearly describe the proposed hosting environment, AI architecture, external services, model providers, security controls, data handling protections, authorization approach, and any dependencies on third-party services. Proposed solutions will be evaluated in accordance with the solicitation requirements.

Q5.12 – AI governance, privacy and records retention - Please identify all privacy, records management, AI governance, data retention, prompt/response logging, model usage, human escalation, and public disclosure requirements applicable to chatbot conversations. | Attachment 1 PWS 3.2, 3.3, and 3.4 Attachment 1 pp. 9-10 / PDF pp. 46-47

A) Offerors shall comply with applicable Federal privacy, records management, cybersecurity, AI governance, and information management requirements, including applicable provisions of OMB Circular A-130, NIST guidance, agency privacy requirements, records management requirements, and any applicable Privacy Impact Assessment (PIA), System of Records Notice (SORN), or related agency policies.

The conversational AI solution shall utilize Government-approved content sources and operate within an SSS-approved content management and governance framework. Government, agency, and end-user data shall not be used to train, fine-tune, or otherwise improve underlying AI models unless expressly authorized in writing by SSS**.**

Section 6 – Hosting, Cloud Infrastructure & Connectivity

Q6.1 – Connectivity architecture - Does SSS require a server-to-server VPN, ExpressRoute, or other dedicated network connection between the contractor-managed hosting environment and SSS internal systems (data center, identity provider, registration system, log endpoints)? | PWS 2.4 / 4.2, 5-6 / 11

A) The solicitation does not prescribe a specific network connectivity architecture or require a particular connection method, such as a server-to-server VPN, ExpressRoute, dedicated circuit, or other private connectivity solution, for proposal purposes.

Offerors should propose an approach that satisfies the security, integration, performance, and operational requirements identified in the PWS. SSS will work collaboratively with the successful contractor after award to provide applicable domain information, identify required integration points, and refine network connectivity, access control, security, and interface requirements necessary to support the contractor-provided solution.

Any required connectivity between the hosting environment and SSS systems, identity services, mission applications, security monitoring capabilities, or other Government resources will be coordinated during implementation planning and execution in accordance with applicable security and operational requirements.

Q6.2 – Azure Government requirement - The Submittal Verification requirements at items 1 and 2 under Factor 2, and PWS sections 2.1 and 4.2, reference AWS services including Amazon S3, Amazon CloudWatch, AWS Certificate Manager, and an SSS to AWS VPN. Amendment 0002 confirms the contractor shall provide a FedRAMP authorized Microsoft Azure Government environment and that AWS is not an option. Please confirm that offerors should propose functionally equivalent Azure Government services in response to these items and that compliance with Submittal Verification item 2 will be evaluated on that basis. Will the Government issue a conforming amendment? | 52.212-1 Addendum, Factor 2 Submittal Verification items 1-2; PWS 2.1, 4.2, Sol. pp. 26-27; PWS pp. 2, 11

A) An Amendment to the RFP clarified that the contractor shall provide and manage a FedRAMP-authorized Microsoft Azure Government hosting environment. AWS is not an acceptable hosting platform for this requirement.

Accordingly, references to specific AWS services in the Submittal Verification requirements should not be interpreted as authorizing or requiring the use of AWS. Rather, offerors shall propose functionally equivalent Microsoft Azure Government services that satisfy the underlying functional, security, monitoring, certificate management, connectivity, logging, and operational requirements identified in the solicitation.

Compliance with the Submittal Verification requirements will be evaluated based on the offeror's ability to demonstrate how its proposed Microsoft Azure Government solution satisfies the applicable requirements. Offerors should clearly map the referenced AWS capabilities to the corresponding Azure Government services included in their proposed solution.

Q6.3 – Azure equivalency guidance - PWS Section 2.1 states the Contractor shall "Provide AWS services including Amazon S3, Amazon CloudWatch, (SSL certificates and Certificate Manager supported by AWS)." Amendment 0001 changes the cloud requirement to Azure. Please confirm that references to AWS-specific services (S3, CloudWatch, Certificate Manager) in PWS 2.1 are superseded by Amendment 0001 and that Offerors should propose the Azure-equivalent services (e.g., Azure Blob Storage, Azure Monitor, Azure Key Vault / App Service Certificates) to satisfy these requirements., Attachment 1, PWS 2.1 (Cloud Infrastructure and Hosting); Amendment 0001, 2 (Attachment 1, Page 2); Amendment 0001

A) Yes. Amendment 0001 and subsequent solicitation amendments clarify that the required hosting environment is Microsoft Azure Government. AWS services are not an acceptable hosting solution for this requirement.

References in PWS 2.1 to AWS-specific services, including Amazon S3, Amazon CloudWatch, AWS Certificate Manager, and other AWS-related technologies, should be interpreted as legacy platform references that are superseded by the Azure Government requirements established through the solicitation amendments.

Offerors shall propose Microsoft Azure Government services and capabilities that satisfy the solicitation's hosting, storage, monitoring, certificate management, security, availability, resiliency, and operational requirements. Examples may include Azure Blob Storage, Azure Monitor, Azure Key Vault, Azure Application Gateway, Azure Web Application Firewall, and other Azure Government services, as appropriate to the offeror's proposed solution.

SSS will evaluate proposed solutions based on compliance with the solicitation requirements and the use of a Microsoft Azure Government hosting environment.

Q6.4 – Web application firewall (WAF) and administrative access - PWS 2.1 requires the contractor to "Build in web Application Firewall (WAF)VPN access for secure administrative operations." Can the government please confirm this requirement intends both (a) a web application firewall protecting public traffic and (b) VPN-restricted access for administrative operations, as two distinct capabilities? Attachment 1 (PWS), Part 2, 2.1 Cloud Infrastructure and Hosting, PWS pg. 2

A) Yes. SSS intends this requirement to encompass both:

• A Web Application Firewall (WAF) or equivalent capability to protect public-facing web services and applications; and

•Secure administrative access controls for authorized personnel, which may include VPN-based access or other approved secure access mechanisms consistent with the solicitation's security requirements. Offerors should describe their proposed approach for satisfying these requirements and supporting secure administration, monitoring, management, and maintenance activities in accordance with the solicitation.

Q6.5 – Domain name system (DNS) and cutover responsibilities - For cutover planning under PWS 4.2, can the government please confirm that SSS retains administrative control of the sss.gov domain through the .gov registrar and will execute DNS changes during the controlled cutover, and identify whether the government or contractor is responsible for TLS certificate issuance for sss.gov in the new environment? Attachment 1 (PWS), Part 4, 4.2 Development Staging, Testing, and Deployment, PWS pg. 11

A) SSS retains ownership and administrative control of the sss.gov domain and will coordinate and execute any required DNS changes associated with the approved cutover process.

For proposal purposes, SSS has not established specific responsibilities regarding TLS certificate issuance, renewal, management, or lifecycle operations for the modernized environment. Offerors should identify any assumptions regarding certificate management, DNS coordination, cutover activities, and related deployment responsibilities in their proposals. SSS will work collaboratively with the successful contractor following award to define domain management, DNS, certificate management, and cutover responsibilities necessary to support transition, testing, deployment, and ongoing operations.

Q6.6 – Azure Government hosting clarification - For cutover planning under PWS 4.2, can the government please confirm that SSS retains administrative control of the sss.gov domain through the .gov registrar and will execute DNS changes during the controlled cutover, and identify whether the government or contractor is responsible for TLS certificate issuance for sss.gov in the new environment? Attachment 1 (PWS), Part 4, 4.2 Development Staging, Testing, and Deployment, PWS pg. 11

A) SSS retains ownership and administrative control of the SSS.gov domain and will coordinate and execute any required DNS changes associated with the approved cutover process. For proposal purposes, SSS has not established specific responsibilities regarding TLS certificate issuance, renewal, management, or lifecycle operations for the modernized environment. Offerors should identify any assumptions regarding certificate management, DNS coordination, cutover activities, and related deployment responsibilities in their proposals. SSS will work collaboratively with the successful contractor following award to define domain management, DNS, certificate management, and cutover responsibilities necessary to support transition, testing, deployment, and ongoing operations.

Q6.7 – Contractor-managed Azure environment - Please confirm whether the Government currently owns an Azure tenant or subscription for this effort, and whether the contractor will deploy into a government-owned Azure environment or a contractor-hosted Azure environment. PWS 2.1, 5.5, Attachment 1, pp. 2 and 14

A) For proposal purposes, SSS has not identified an existing Government-owned Azure tenant, subscription, landing zone, or hosting environment that offerors should assume will be provided for this effort. The solicitation requires the contractor to provide and manage a FedRAMP-authorized Microsoft Azure Government hosting environment that satisfies the requirements of the solicitation. Offerors should propose a solution consistent with those requirements and clearly identify any assumptions regarding tenant ownership, subscription management, hosting responsibilities, access controls, and operational support.

SSS will work collaboratively with the successful contractor after award to provide available information regarding tenant configuration, access requirements, transition planning, and implementation activities, as appropriate.

Section 7 – Website Scope, CMS & Architecture

Q7.1 – Website modernization scope - The PWS describes a “static website,” but also includes requirements such as CMS, secure login/MFA, Azure AD/Entra ID integration, and user-facing capabilities (e.g., ability for end-users to update registration records and upload documentation). Please clarify whether these application-like capabilities are in scope for this effort and whether they are expected to be delivered within the website solution or via integration to an existing SSS application.

A) The primary objective of this effort is modernization of the public-facing website and supporting content management capabilities. User-facing application functionality, such as registration updates, document submission, authentication, and related business processes, may be provided through integration with existing or future Selective Service

System applications and services. Offerors should propose a solution that supports secure integration with such capabilities where required. The solicitation does not require the development of standalone registration, records management, or automatic registration applications unless otherwise specifically identified.

Q7.2 – CMS flexibility - PWS Section 2.2 states the Contractor shall "Integrate a WordPress or an equivalent content management system (CMS)." Does the Government consider a fully custom-developed CMS, purpose-built by the Contractor specifically for this engagement and deployed within the FedRAMP-authorized Azure Government environment, to qualify as an "equivalent" CMS under this requirement? A custom-built CMS would eliminate third-party plugin vulnerabilities, be developed under NIST SP 800-218 secure development practices, and fall entirely within the system's Authority to Operate (ATO) boundary., Attachment 1, PWS 2.2 (Website Design and Platform Requirements), 3 (Attachment 1, Page 3)

A) SSS does not require the use of a specific content management system product, architecture, or technology stack beyond the requirements identified in the solicitation.

Offerors may propose a WordPress implementation or an alternative content management solution, including a custom-developed CMS, provided the proposed solution satisfies the solicitation's functional, security, accessibility, content management, maintainability, scalability, and operational requirements.

Offerors should clearly describe their proposed CMS approach and demonstrate how it provides capabilities equivalent to those expected of an enterprise content management system, including content authoring and publishing, workflow support, user administration, auditability, security, training, maintainability, and long-term support. SSS will evaluate proposed solutions in accordance with the solicitation requirements and evaluation criteria.

Q7.3 – CMS security management - If a custom-developed CMS is acceptable under PWS 2.2, how should the Offeror address Submittal Verification Item 5, "Provide CMS and Plugin Security Management" (Section 52.212-1 Addendum, Factor 2b)? Specifically, for a custom CMS that has no third-party plugins, should the Offeror address this requirement by describing its approach to component and dependency security management (e.g., automated dependency scanning, SBOM generation, secure coding practices) in lieu of traditional plugin management? Section 52.212-1 Addendum, Factor 2b, Submittal Verification Item 5, 26

A) Yes. Offerors proposing a content management solution that does not utilize traditional CMS plugins should address the underlying intent of the requirement rather than plugin management specifically.

For custom-developed CMS solutions or other architectures that do not rely on third-party plugins, offerors should describe their approach to managing the security of software components, dependencies, integrations, libraries, application updates, and other elements of the proposed solution. This may include practices such as secure software development, vulnerability management, dependency management, software composition analysis, software bill of materials (SBOM) management, patch management, software supply chain risk management, code review, and continuous monitoring.

SSS will evaluate compliance with Submittal Verification Item 5 based on the offeror's ability to demonstrate a sound approach for maintaining the security, integrity, supportability, and ongoing maintenance of the proposed CMS solution, regardless of the specific technology architecture employed.

Q7.4 – Makon/MakonCloud clarification - Amendment 0001 introduces references to "Makon," "MakonCloud," and "MakonLoud" in the context of CMS and cloud hosting. Please clarify: (a) Are these references identifying a specific required CMS platform, or are they examples of acceptable solutions? (b) Does the Government mandate use of a specific CMS product, or does the "or equivalent" language in PWS 2.2 remain in effect, permitting Offerors to propose any CMS solution (including custom-built) that meets all functional, security, and compliance requirements of the PWS?, Amendment 0001; Attachment 1, PWS 2.1 and 2.2, Amendment 0001, Page 1; Attachment 1, Pages 2-3

A) The references to "Makon," "MakonCloud," and "MakonLoud" are not intended to mandate a specific CMS platform, hosting provider, cloud service, or proprietary product, nor do they establish a preferred solution.

The "WordPress or an equivalent content management system (CMS)" language in PWS 2.2 remains in effect. Offerors may propose WordPress or an alternative CMS solution, including a custom-developed CMS, provided the proposed solution satisfies the functional, security, accessibility, hosting, content management, maintainability, and compliance requirements identified in the solicitation.

Offerors are responsible for demonstrating how their proposed solution satisfies the solicitation requirements. Proposed solutions will be evaluated in accordance with the solicitation requirements and evaluation criteria.

Q7.5 – Website versus mission-system responsibilities -The PWS references functionality such as registration updates, document uploads, identity verification, user authentication, and other user interactions. Please clarify which capabilities are expected to be provided by the contractor-developed website and which will be handled by existing or future Selective Service System mission systems.

A) The modernized website will serve as the Selective Service System's public-facing website and content management platform. Registration updates, document uploads, identity verification, authentication, and other mission-system functions will be provided through existing or future SSS applications, as applicable.

The modernized website will integrate with those systems through approved interfaces, embedded services, APIs, links, or other mechanisms. Offerors should propose solutions that support secure integration while maintaining a seamless user experience.

Q7.6 – Authentication and identity management - Please clarify whether public registrants and end users are required to authenticate through the contractor-provided website and identify any required identity assurance levels or authentication standards.

A) Public registrants and end users are not required to authenticate through the contractor-provided website. Authentication, identity proofing, registration updates, document uploads, and related transaction processing are provided through existing or future Selective Service System mission systems, as applicable.

Offerors are not required to propose a separate public-facing identity-proofing or authentication solution for the modernized website. Accordingly, SSS is not establishing specific Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), or identity-proofing provider requirements for the contractor-provided website as part of this solicitation.

Offerors should propose solutions consistent with the solicitation requirements and applicable Federal security standards.

Q7.7 – Hosting architecture and cloud environment - Does SSS require the modernized website to be hosted in a Government-owned environment, or may offerors propose a contractor-managed hosting environment?

A) The solicitation contemplates a contractor-provided hosting environment during contract performance. Offerors shall provide and manage a hosting environment that satisfies the solicitation's security, availability, performance, compliance, and operational requirements.

The transition-out requirements are intended to ensure the orderly transfer of website assets, configurations, documentation, data, and related materials to a Government-designated environment or successor contractor at the conclusion of performance.

Q7.8 – Conversational AI integration - Does SSS intend for the conversational AI capability to function as an independent chatbot platform or as an integrated component of the modernized website?

A) The conversational AI capability shall function as an integrated component of the modernized website experience and support public-facing information and guidance related to Selective Service System programs and services.

The conversational AI solution shall utilize Government-approved content sources and operate within an SSS-approved content management and governance framework. The solution is expected to support activities such as answering frequently asked questions, providing navigation assistance, directing users to appropriate resources, and assisting users in locating publicly available information.

The conversational AI solution is not intended to replace existing mission systems or provide direct access to registration records or other personalized mission-system data unless otherwise specifically authorized by SSS.

Q7.9 – Integration architecture flexibility - The PWS references integration through APIs, embedded services, and iframe-based approaches. Does SSS require a specific integration architecture?

A) SSS has not prescribed a specific integration architecture. Offerors may propose an approach that satisfies the solicitation's functional, security, accessibility, performance, maintainability, and user experience requirements.

Integration may involve APIs, service endpoints, embedded services, iframes, links, or other approved mechanisms, as appropriate. Proposed solutions will be evaluated in accordance with the solicitation requirements and evaluation criteria.

Section 8 – Federal Digital Experience, Accessibility & Design Standards

Q8.1 – USWDS and Federal standards - Does the Government require the use of the U.S. Web Design System (USWDS) for the website design? The RFP references 21st Century IDEA and America by Design but does not explicitly require USWDS. | PWS 2.5, 6

A) Yes. Offerors shall utilize the U.S. Web Design System (USWDS) in the design and development of the modernized website. The solution shall comply with applicable Federal website and digital service requirements, including the Federal Website Standards, the 21st Century Integrated Digital Experience Act (21st Century IDEA), and

OMB Memorandum M-23-22, Delivering a Digital-First Public Experience. Offerors may propose implementation approaches that leverage USWDS while meeting the functional, accessibility, usability, branding, and content management requirements of the solicitation.

Q8.2 – America by Design compliance requirements - The PWS references compliance with the Executive Order "America by Design" and related requirements for improving visual presentation, usability, and user experience. Can SSS provide a specific checklist or compliance framework that offerors should address as part of their proposal? | PWS 2.5, 6

A) Offerors shall comply with the requirements identified in the solicitation and applicable Federal digital experience, accessibility, usability, and website design standards, including the 21st Century IDEA, Federal Website Standards, U.S. Web Design System (USWDS), OMB Memorandum M-23-22, and other referenced guidance.

SSS does not intend to provide a separate "America by Design" compliance checklist. Offerors should describe their approach to meeting applicable requirements and best practices related to user experience, accessibility, usability, visual design, content presentation, mobile responsiveness, and digital service delivery.

For purposes of this requirement, America by Design compliance is limited to the scope of the website modernization effort and associated digital services. Broader Agency-wide customer experience initiatives outside the scope of this contract are not required unless otherwise specified in the solicitation.

Q8.3 – Branding, design standards, and visual identity - Does SSS have existing branding standards, visual identity guidelines, design system requirements, component libraries, or other design assets that the Contractor must follow as part of the website modernization effort? | PWS 2.2; PWS 4.1, 40, 47-48

A) Offerors shall comply with applicable Federal digital experience, accessibility, and design requirements, including the U.S. Web Design System (USWDS), Federal Website Standards, 21st Century IDEA, OMB Memorandum M-23-22, and other solicitation requirements. SSS will provide available branding, visual identity, content, style guidance, and other relevant Government-furnished information following award, as appropriate. Offerors should describe their approach to supporting Agency branding, accessibility, usability, mobile-first design, content presentation, and user-centered design requirements.

Specific decisions regarding branding implementation, design components, navigation structures, content presentation, and visual identity will be refined through the discovery, design, and Government review processes during contract performance.

Section 9 – Content Governance, Migration & Government-Furnished Information

Q9.1 – Migration assumptions - Can the Government provide an estimate of the total number of content pages, documents, media assets, and structured data records anticipated for migration? Additionally, are there known content quality, taxonomy, metadata, or records management considerations that should be factored into migration planning?

A) SSS has not established a definitive inventory of website content, documents, media assets, structured data, metadata, taxonomy elements, or records management attributes for proposal purposes. Offerors should assume that discovery, assessment, content analysis, and migration planning activities will be required as part of the modernization effort. The scope and prioritization of content migration, remediation, metadata management, taxonomy refinement, and records management considerations will be determined during implementation.

Q9.2 – Government-furnished information - Will SSS provide a list of Government-Furnished Information (GFI) including existing content files, brand guidelines, system documentation, or other materials? When will this GFI be made available after award? | PWS 4.1 / 2.9, 8 / 11

A) The Government anticipates providing available Government-Furnished Information (GFI) relevant to contract performance, which may include website content, technical documentation, interface documentation, branding guidance, system information, and other available materials. The specific GFI package and timing of delivery will be coordinated with the successful Contractor following award.

Q9.3 – Content ownership, approval authority, and publishing controls - Please clarify content ownership, content approval authority, and publishing responsibilities following implementation. Will contractor personnel be authorized to publish content directly to production, or will all content publication require SSS review and approval? | PWS 2.2; PWS 2.9

A) SSS retains ownership of all website content and maintains final approval authority for content publication.

The Contractor shall provide content management, workflow, governance, and publishing capabilities that support SSS review, approval, and publication processes. Contractor personnel may support content migration, content preparation, content maintenance, workflow administration, and related activities as authorized by SSS.

Specific publishing permissions, workflow approvals, user roles, and content governance processes will be established collaboratively with the successful Contractor following award.

Q9.4 – Content modernization - Please clarify whether SSS will provide final approved content for migration, or whether the contractor should assume responsibility for content editing, plain language refinement, consolidation recommendations, and rewrite support. | PWS 2.9, 8

A) SSS will provide existing website content and will work collaboratively with the successful contractor to identify content that should be migrated, retained, archived, consolidated, updated, or retired as part of the modernization effort.

Offerors should assume responsibility for supporting content migration activities and may recommend content improvements, plain language enhancements, content restructuring, accessibility updates, consolidation opportunities, and other modernization recommendations consistent with their proposed approach. Final content approval and publication authority will remain with SSS. The solicitation does not prescribe the extent of content editing, rewriting, or content governance activities for proposal purposes. Specific content migration, review, refinement, and approval processes will be coordinated with the successful contractor during implementation planning and execution.

Q9.5 – Migration pricing assumptions - Amendment 0002, Response A10 states that "The appropriate volume of pages, documents, media, and forms will be provided." Given that this is a firm-fixed-price requirement and migration scope under PWS 2.9 is a significant cost driver, can the government please provide the approximate volume of pages, documents, media files, and forms in scope for migration prior to the proposal due date? If volumes cannot be provided prior to the due date, can the government please confirm that offerors may include reasonable bounding assumptions regarding migration volume without such assumptions being considered grounds for rejection under the assumption provisions? PWS 2.9; A10; 52.212-1/52.212-2 assumption provisions, PWS pgs. 7–8, pgs. 27, 37

A) SSS acknowledges that content migration volume is an important consideration in proposal development and pricing.

As noted elsewhere in the solicitation and amendments, SSS intends to provide available content inventory information. However, SSS may not provide a complete or detailed inventory of all pages, documents, media assets, forms, and related content prior to proposal submission.

If detailed migration volumes are not provided prior to proposal submission, offerors may identify reasonable assumptions regarding the volume and complexity of pages, documents, media assets, forms, and related content included in their proposals.

Any assumptions should be clearly stated, consistent with the solicitation requirements, and sufficient to support the offeror's proposed technical approach and pricing. Clearly identified assumptions will be evaluated in accordance with the terms of the solicitation.

Q9.6 – Current website platform, analytics, and content inventory - Please provide information regarding the current website platform, hosting environment, CMS technology, analytics tools, content inventory, and incumbent support arrangements. Will existing analytics exports, content inventories, or migration-related documentation be provided to the successful contractor? | PWS 2.9; Amendment 0002, A10

A) Following award, SSS will provide available Government-furnished information, documentation, analytics information, content inventories, migration-related materials, system information, and other resources necessary to support contract performance, as appropriate.

SSS does not currently plan to provide detailed information regarding the current website platform, hosting environment, CMS technology, analytics configuration, content inventories, or incumbent support arrangements during the solicitation period.

Offerors should identify any assumptions regarding migration scope, content volume, analytics availability, hosting, transition activities, or content governance within their proposals.

Section 10 – Identity Management, APIs & Integrations

Q10.1 – Integration assumptions - System Integrations- Are there existing or planned integrations with identity management, HR systems, records management systems, or workforce readiness platforms that should be considered during modernization planning?

A) SSS anticipates integration with existing enterprise services, including identity and access management capabilities, and may require integration with additional Government systems during contract performance. The Government has not established a definitive inventory of current or future integrations for proposal purposes. Offerors should propose a flexible, secure integration approach that supports future interoperability requirements.

Q10.2 – Scope limitations - The PWS describes a “static website,” but also includes requirements such as CMS, secure login/MFA, Azure AD/Entra ID integration, and user-facing capabilities (e.g., ability for end-users to update registration records and upload documentation). Please clarify whether these application-like capabilities are in scope for this effort and whether they are expected to be delivered within the website solution or via integration to an existing SSS application.

A) The primary objective of this effort is modernization of the public-facing website and supporting content management capabilities. User-facing application functionality, such as registration updates, document submission, authentication, and related business processes, may be provided through integration with existing or future Selective Service System applications and services. Offerors should propose a solution that supports secure integration with such capabilities where required. The solicitation does not require the development of standalone registration, records management, or automatic registration applications unless otherwise specifically identified.

Q10.3 – Connectivity and integrations - Does SSS require a server-to-server VPN, ExpressRoute, or other dedicated network connection between the contractor-managed hosting environment and SSS internal systems (data center, identity provider, registration system, log endpoints)? | PWS 2.4 / 4.2, 5-6 / 11

A) The solicitation does not prescribe a specific network connectivity architecture or require a particular connection method, such as a server-to-server VPN, ExpressRoute, dedicated circuit, or other private connectivity solution, for proposal purposes.

Offerors should propose an approach that satisfies the security, integration, performance, and operational requirements identified in the PWS. SSS will work collaboratively with the successful contractor after award to provide applicable domain information, identify required integration points, and refine network connectivity, access control, security, and interface requirements necessary to support the contractor-provided solution.

Any required connectivity between the hosting environment and SSS systems, identity services, mission applications, security monitoring capabilities, or other Government resources will be coordinated during implementation planning and execution in accordance with applicable security and operational requirements.

Q10.4 – Government-managed integration endpoints - Amendment 0002 references integration with five Government-managed endpoints. Please identify the endpoints and clarify whether detailed interface documentation, testing resources, and technical requirements will be provided prior to implementation. | PWS 3.1; Amendment 0002

A) SSS has identified multiple Government-managed integration endpoints that support mission and enterprise functions. Detailed interface documentation, technical requirements, testing resources, available environments, endpoint ownership information, and integration guidance will be provided to the successful Contractor following award, as appropriate.

Offerors should base their proposals on the integration requirements identified in the solicitation and propose a flexible architecture capable of supporting secure integration with Government-managed services.

Q10.5 – Integration methods and architecture flexibility - PWS 3.1 references integration with existing Government applications. Please confirm whether SSS requires a specific integration approach, such as APIs, embedded applications, iFrames, service endpoints, or other mechanisms. | PWS 3.1

A) SSS does not prescribe a specific integration architecture for proposal purposes.

Offerors may propose APIs, service endpoints, embedded services, iFrames, or other secure integration mechanisms that satisfy the solicitation's functional, security, accessibility, maintainability, and user experience requirements. Proposed solutions will be evaluated in accordance with the solicitation requirements.

Q10.6 – Identity and authentication responsibilities- Please clarify whether the modernized website is responsible for performing authentication, identity proofing, registration updates, or document submission processing for public users. | PWS 2.1; PWS 2.2; PWS 3.1

A) Public registrants and end users are not required to authenticate through the contractor-provided website.

Authentication, identity proofing, registration updates, document uploads, and related transaction processing are provided through existing or future Selective Service System mission systems, as applicable. The modernized website shall provide secure access to and integration with those systems through approved interfaces, embedded services, APIs, links, or other mechanisms as required.

Offerors are not required to propose a separate public-facing identity-proofing or authentication solution as part of the website modernization effort.

Q10.7 – Authoritative systems of record - Please identify the authoritative systems of record for registration-related data and clarify whether the Contractor is expected to develop registration processing capabilities. | PWS 3.1

A) Existing Selective Service System mission systems remain the authoritative systems of record for registration-related data, processing, and business functions.

The Contractor is not expected to replace or redevelop registration systems, registration logic, or mission processing capabilities. The Contractor shall provide integration with existing Government-managed systems and services as required by the solicitation.

Section 11 – AI Conversational FAQ & Information Assistance

Bottom Line Up Front: The AI Conversational Interface is intended to provide FAQ support and information assistance using SSS-approved content. The chatbot is not intended to provide:

- Personalized data retrieval
- Transaction processing
- Registration-record management
- Unrestricted internet retrieval

Q11.1 – Chatbot governance - Factor 2.b Submittal Verification Item 17 requires "documentation that the Chatbot solution is FedRAMP-authorized." PWS Section 3.2 states the chatbot shall be "FedRAMP-authorized or otherwise formally approved by the Agency for use within the SSS.gov environment." Please reconcile these provisions: is an Agency-approved (but not FedRAMP-authorized) chatbot acceptable at proposal submission, and if so, what is the Agency-approval pathway, approving authority, and expected timeline? | Section M / Factor 2.b, Item 17; PWS Section 3.2, 27, 46

A) The chatbot solution must be FedRAMP-authorized. SSS will collaborate with the vendor to develop agency-approved content and messaging that will be housed in a secure sandbox environment accessible to the chatbot. In addition, SSS will work with the vendor to establish agency-approved communication tree configurations that enable customers to easily navigate and obtain the information they need.

Q11.2 – FedRAMP AI services - Will the use of existing FedRAMP-authorized AI services (e.g., Azure OpenAI Service [FedRAMP High], AWS Bedrock [FedRAMP Moderate]) satisfy the requirement, or is a separately authorized AI system required within the solution boundary? AI Conversational Capability (3.2–3.4); AI / CONVERSATIONAL INTERFACE REQUIREMENTS, 46-47

A) Offerors may propose the use of FedRAMP-authorized AI services that satisfy the solicitation's security, privacy, accessibility, hosting, and functional requirements.

SSS has not prescribed a specific authorization approach for AI components. Offerors should clearly describe their proposed architecture, authorization boundary, security controls, hosting approach, and compliance methodology, including how AI services are incorporated into the overall solution and supporting authorization package. Proposed solutions will be evaluated in accordance with the solicitation requirements.

Q11.3 – AI data governance - Can SSS confirm whether AI models may be trained or fine-tuned using SSS-provided content, or must usage remain inference-only? AI Data Governance (3.2); AI / CONVERSATIONAL INTERFACE REQUIREMENTS, 46

A) No. AI models shall not be trained, fine-tuned, retained for model improvement, or otherwise improved using Government, Agency, or end-user data unless expressly authorized in writing by SSS. Offerors should assume the conversational AI solution will operate using Government-approved content and knowledge sources and should describe how their proposed solution complies with the solicitation's data protection, privacy, security, and AI governance requirements.

Q11.4 – AI content sources - Will SSS provide written authorization to use SSS-generated FAQs, user guides, and public-facing documentation to build the chatbot? AI Data Governance (3.2); AI / CONVERSATIONAL INTERFACE REQUIREMENTS, 46

A) SSS may provide approved public-facing content, including FAQs, website content, user guidance, informational materials, policy information, and other Agency-approved content sources for use in configuring, populating, and supporting the conversational AI solution.

The conversational AI solution is expected to use Government-approved content sources as the basis for responses provided to users. Any use of Government content shall comply with the solicitation's AI governance, privacy, security, and data protection requirements Additional information regarding approved content sources, formats, and governance requirements will be coordinated with the successful Contractor following award.

Q11.5 – AI use cases - Can SSS provide examples or use cases illustrating the expected AI chatbot complexity: (a) simple FAQ responses; (b) multi-step workflow guidance; or (c) backend system integration for personalized data retrieval? AI Data Governance (3.2); AI / Conversational Interface Requirements, 46

A) The conversational AI solution is expected to support public-facing information and guidance related to Selective Service System programs, services, and website content. Representative use cases may include answering frequently asked questions, providing navigation assistance, directing users to appropriate resources, assisting users in locating information, and guiding users through publicly available processes and services.

The conversational AI solution is expected to provide responses based on Government-approved content and knowledge sources. SSS does not currently anticipate direct access to personalized user data, transaction processing, or unrestricted internet-based information retrieval through the conversational AI solution unless otherwise specified.

Q11.6 – AI review and approval requirements - PWS 3.2 requires the chatbot solution to comply with "all applicable federal cybersecurity, privacy, and artificial intelligence governance requirements, including OMB guidance related to AI use," and PWS 3.4 states implementation shall not proceed until all government security, privacy, and governance approvals are obtained. Can the government please identify the specific OMB AI governance memoranda applicable to this requirement (e.g., M-25-21, M-25-22) and describe the Agency's AI approval process and anticipated approval timeline, so offerors can incorporate this dependency into the project schedule required under Factor 1? Attachment 1 (PWS), Part 3, 3.2 and 3.4, PWS pgs. 9–10

A) SSS requires compliance with all applicable Federal cybersecurity, privacy, artificial intelligence, records management, and governance requirements in effect at the time of contract performance.

For proposal purposes, SSS is not providing a definitive list of applicable OMB memoranda, agency-specific AI governance requirements, or approval timelines. Offerors should propose an approach that accommodates Government review, risk assessment, security, privacy, accessibility, and governance activities associated with the implementation of chatbot or AI-enabled capabilities.

Implementation of chatbot functionality shall be subject to applicable Government security, privacy, and governance approvals as required by the solicitation. Offerors should account for these review and approval activities in their proposed schedules. Additional guidance regarding applicable requirements, approval processes, roles, and responsibilities will be provided following award, as appropriate.

Q11.7 – Chatbot internet access and external content - Will the conversational AI solution be permitted to retrieve information from the public internet or external data sources at runtime, or must responses be limited to Government-approved content sources? | PWS 3.2–3.4

A) The conversational AI solution is intended to provide information assistance using Government-approved content and knowledge sources. Offerors should assume that chatbot responses will be generated from content approved by SSS and maintained within the approved knowledge base and content management process.

The solicitation does not require unrestricted internet access, external web retrieval, or dynamic retrieval of information from public internet sources. Any use of external content sources would be subject to SSS review, approval, security requirements, privacy requirements, and applicable AI governance requirements.

Q11.8 – Chatbot response approval and content management - Will SSS participate in the development, review, and approval of chatbot messaging, conversation flows, escalation paths, and knowledge-based content? | PWS 3.2–3.4

A) Yes. SSS will work collaboratively with the successful Contractor to develop, review, refine, and approve chatbot messaging, communication tree structures, escalation workflows, response libraries, and knowledge-based content.

The conversational AI solution is expected to operate using content approved by SSS. Final approval authority for chatbot content, messaging, user guidance, escalation pathways, and public-facing responses will remain with SSS.

Q11.9 – Human escalation and customer support routing - Does SSS require the conversational AI solution to support escalation to human assistance when the chatbot cannot answer a question or when users require additional support? | PWS 3.2–3.4

A) Yes. Offerors should provide an approach that supports escalation to appropriate SSS resources, contact methods, support channels, or other Government-approved assistance mechanisms when users require additional support beyond the chatbot's capabilities.

Specific escalation workflows, routing procedures, support channels, communication trees, and operational processes will be coordinated with the successful Contractor during implementation.

Q11.10 – Chatbot source transparency - Does SSS require the chatbot to cite source documents when responding to users? | PWS 3.2–3.4

A) SSS encourages the use of authoritative and Government-approved content sources in support of chatbot responses. Offerors should describe their approach to transparency, source management, response traceability, and content governance.

The solicitation does not currently require chatbot responses to display citations to specific source documents; however, the proposed solution should support the use of approved content sources and maintain traceability to the underlying approved knowledge base.

Section 12 – Testing, Training & Acceptance

12.1 – Penetration testing - Please clarify whether penetration testing is required for only new automatic registration components and APIs, or for the full website, CMS, chatbot, hosting environment, staging environment, and integrations. | Attachment 1 PWS 2.4 and 3.1, Attachment 1 pp. 4-6, 8-9 / PDF pp. 41-43, 45-46

A) SSS expects penetration testing to encompass the complete modernized web solution and all associated components that are part of the contractor-provided environment or

integrated solution. This includes, at a minimum, the public-facing website, content management system (CMS), AI chatbot and related interfaces, APIs, authentication and access control mechanisms, hosting environment, supporting infrastructure, administrative interfaces, and all integrations that are within the scope of the modernization effort

To the extent that staging, development, test, and production environments are part of the contractor's solution, the contractor shall implement appropriate security testing activities for those environments consistent with industry best practices and applicable federal security requirements. The Government's intent is to ensure that security vulnerabilities are identified and remediated across the entire solution stack rather than limiting testing solely to new automatic registration components or APIs.

However, offerors are not expected to perform penetration testing against Government-owned legacy mission systems that are outside the scope of the website modernization effort. For integrations with existing SSS systems, testing should focus on the security of the interfaces, data exchanges, authentication mechanisms, and integration points that are part of the proposed solution. The contractor shall coordinate with SSS regarding any testing activities that could affect operational systems or require specific authorization.

Q12.2 – Training requirements - Approximately how many SSS staff will require administrator or editor training on the new CMS, and how many end-user training sessions are anticipated?

A) SSS has not established a definitive number of CMS administrators, content editors, approvers, or other users requiring training for proposal purposes. Offerors should propose a training approach that supports successful adoption and administration of the solution. The number of trainees, training sessions, and associated training requirements will be finalized during implementation planning in coordination with the successful Contractor.

Q12.3 – Acceptance readiness - Please clarify the acceptance criteria for “substantially completed” by September 25, 2026, including whether this means production deployment, UAT completion, security approval, content migration completion, ATO approval, training completion, and closeout. Technical Capability and Project Schedule, PWS 7.1, Solicitation p. 25 and Attachment 1, pp. 16 to 17

A) For proposal purposes, "substantially completed" means that the modernized website solution is functionally complete and ready for transition to production operations by September 25, 2026. At a minimum, SSS expects core development, testing, content migration, training, and user acceptance activities necessary to support deployment readiness to be substantially complete.

The solicitation does not establish detailed acceptance criteria or mandatory completion milestones for individual activities such as production deployment, final content migration, training completion, security authorization issuance, contract closeout, or other post-implementation activities. SSS will work collaboratively with the successful contractor after award to refine implementation milestones, deployment readiness criteria, testing requirements, authorization activities, and transition planning.

Q12.4 – Environment requirements - Beyond Production and Staging (mentioned in the PWS), are additional non-production environments required (e.g., separate UAT, training, demo, or developer sandbox environments)? | PWS 2.1 / 4.2, 2-3 / 11

A) The solicitation expressly requires Production and Staging environments. SSS has not established requirements for separate User Acceptance Testing (UAT), training, demonstration, development, or sandbox environments for proposal purposes.

Offerors may propose additional non-production environments if they believe such environments are necessary to support their implementation, testing, deployment, training, security, or operational approach. Any additional environment requirements, configurations, access controls, and operational procedures will be refined and coordinated with the successful contractor during implementation planning and execution.

Q12.5 – Government review and approval timelines - Please provide expected Government review and approval turnaround times for discovery deliverables, design packages, security documentation, AI governance submissions, UAT results, training materials, production readiness packages, and other required deliverables. | PWS 4.1; PWS 4.2; PWS 7.1

A) SSS will make reasonable efforts to review and provide feedback on discovery deliverables, design packages, security documentation, AI governance submissions, testing results, training materials, production readiness artifacts, and other required deliverables in a timely manner.

SSS has not established specific review or approval turnaround times for proposal purposes. Offerors should propose a realistic project schedule that includes adequate time for Government reviews, comments, revisions, testing activities, and approval processes.

Q12.6 – User Acceptance Testing responsibilities - Please clarify the respective responsibilities of SSS and the Contractor during User Acceptance Testing (UAT), including test planning, test script development, defect management, retesting, and final acceptance. | PWS 4.2; PWS 7.1

A) The Contractor shall support testing activities necessary to demonstrate that the solution satisfies the requirements of the solicitation. This includes preparation of testing materials, coordination of testing activities, support for defect resolution, retesting, and other activities necessary to support deployment readiness.

SSS will participate in User Acceptance Testing and will provide review, feedback, and acceptance determinations consistent with the implementation approach developed after award. Specific testing roles, responsibilities, procedures, and acceptance processes will be coordinated with the successful Contractor during implementation planning.

Q12.7 – Cutover readiness and deployment timing - Please clarify whether the September 25, 2026 substantial completion milestone requires production cutover by that date or whether SSS may accept a solution that is deployment-ready and awaiting final Government approval or cutover activities. | PWS 7.1; PWS 7.2; Amendment 0002

A) For proposal purposes, SSS may accept a solution that is fully tested, deployment-ready, and "cutover ready" by September 25, 2026, provided all required implementation, testing, migration, training, security, and deployment-readiness activities have been substantially completed. Final production cutover activities, final authorization activities, or other Government-directed deployment actions may occur in accordance with the approved implementation and transition plan. Offerors should propose a realistic schedule that supports achievement of deployment readiness by the required milestone date.

Q12.8 – Independent third-party assessments - Amendment 0002 requires penetration testing to be performed by an independent third party. Please clarify whether the Contractor is responsible for procuring and funding the assessor. | Amendment 0002

A) Unless otherwise clarified through a solicitation amendment, offerors should assume that all costs necessary to satisfy the solicitation requirements, including required independent third-party security assessments, penetration testing, validation activities, and associated reporting, are included in their proposed pricing.

Section 13 – Operations, Sustainment & Transition

Q13.1 – Transition-out support - Please confirm whether transition-out support under CLIN 6001 should be priced as an optional CLIN, included in the base price, or priced only if separately exercised. CLIN 6001, PWS 5.5, Solicitation p. 9 and Attachment 1, pp. 13 to 14

A) CLIN 6001 is identified as a separate CLIN for transition-out support. Offerors should provide pricing for CLIN 6001 in accordance with the solicitation's pricing instructions and should not include transition-out support costs within the base contract pricing unless otherwise reflected in their proposed pricing structure.

SSS has not established a specific quantity, labor-hour estimate, or exercise date for transition-out activities. Offerors should develop reasonable assumptions and provide sufficient supporting detail to allow evaluation of the proposed pricing.

Transition-out support will be performed only if required by SSS and in accordance with the terms of the contract. Offerors should clearly identify any assumptions used in developing their proposed pricing for CLIN 6001.

Q13.2 – Operations and sustainment period of performance - Please confirm whether operations and sustainment activities begin upon substantial completion of the website modernization effort and whether they are performed under a separate CLIN and period of performance. | PWS Parts 5-7; CLIN Structure; Amendment 0002

A) Yes. The website modernization and implementation effort is separate from ongoing operations and sustainment activities.

The September 25, 2026 substantial-completion milestone applies to implementation, modernization, testing, migration, integration, deployment readiness, training, and related activities necessary to achieve the project objectives.

Operations and sustainment activities will be performed under their respective contract line items and contract periods beginning after implementation activities are completed and accepted by SSS.

Q13.3 – Contractor-hosted environment during operations - Please confirm whether the production website environment will remain contractor-hosted during the base period and option periods. | PWS 2.1; PWS 5.5; Amendment 0001

A) The solicitation contemplates a contractor-provided hosting environment during contract performance.

Unless otherwise directed by SSS, the contractor shall provide, operate, secure, maintain, monitor, and support the hosting environment necessary to satisfy the requirements of the contract throughout the applicable performance period.

Transition-out requirements are intended to support an orderly transfer of assets, documentation, configurations, data, and related materials to SSS or a successor contractor at the conclusion of performance.

Q13.4 – Operations, maintenance, and enhancement requests - During the operations and sustainment period, will the contractor be responsible solely for maintenance and support activities, or should offerors anticipate ongoing enhancements and feature updates? | PWS Part 5; CLIN 0003

A) During the operations and sustainment period, the contractor shall provide support, maintenance, monitoring, troubleshooting, patching, security updates, content management support, and other activities identified in the solicitation.

SSS may request enhancements, modifications, improvements, or additional capabilities during contract performance in accordance with the contract structure and applicable CLINs. The specific scope of future enhancements cannot be determined for proposal purposes.

Q13.5 – Transition-out deliverables - Please clarify the expected transition-out deliverables at the conclusion of contract performance. | PWS 5.5

A) Transition-out activities are intended to support an orderly transfer of operational responsibility to SSS or a successor contractor.

Expected transition-out deliverables may include system documentation, architecture documentation, source code, configuration information, content assets, deployment procedures, operational procedures, security documentation, administrative credentials, knowledge transfer activities, and other materials necessary to support continuity of operations.

Specific transition requirements will be coordinated with the contractor at the time transition activities are initiated.

Q13.6 – Service level applicability - Please clarify whether uptime, monitoring, and operational support requirements apply only to the public website or to all contractor-managed solution components. | PWS 2.7; PWS 8.1

A) Operational, monitoring, availability, security, and support requirements apply to the contractor-managed solution and all components necessary to support delivery of the required services.

This includes the public website, content management system, hosting environment, administrative interfaces, chatbot components, integrations, APIs, monitoring capabilities, logging capabilities, and other contractor-managed solution components required for contract performance.

Section 14 – Small Business Participation

Q14.1 – Small business participation calculation - Please confirm whether the Small Business Participation Commitment Document requirement applies to small business primes and whether a small business prime may count its own performance toward the 30 percent minimum quantitative requirement. Volume V Contract Documentation, Solicitation p. 29

A) Yes. The Small Business Participation Commitment Document requirement applies to all offerors, including small business prime offerors.

For purposes of satisfying the solicitation's Small Business Participation requirement, a small business prime offeror may count its own performance toward the minimum quantitative participation requirement. Offerors should clearly identify the percentage of work to be performed by the prime contractor and any participating subcontractors, as applicable, in accordance with the solicitation instructions.

Q14.2 – Small business subcontracting requirements - Please confirm whether a small business prime is required to submit a Small Business Subcontracting Plan, or only the Small Business Participation Commitment Document. | Volume V Contract Documentation, Solicitation pp. 29 to 30

A) Small business prime offerors are not required to submit a Small Business Subcontracting Plan. However, all offerors, including small business prime offerors, shall comply with the solicitation's Small Business Participation requirements and submit the required Small Business Participation Commitment Document identified in Volume. Offerors should review the solicitation instructions and applicable contract documentation requirements to ensure all required representations, certifications, and participation commitments are included with their proposals.

Q14.3 – Use of subcontractors to satisfy participation goals - May offerors satisfy the Small Business Participation requirement through a combination of prime contractor performance and subcontractor participation? | Volume V Contract Documentation

A) Yes. Offerors may satisfy the Small Business Participation requirement through a combination of work performed by the prime contractor and work performed by qualifying small business subcontractors.

Offerors should clearly identify the percentage of work to be performed by the prime contractor and each participating small business subcontractor in accordance with the solicitation instructions and Small Business Participation Commitment Document.

Q14.4 – Evaluation of small business participation commitments - Will proposed small business participation percentages be evaluated as part of the proposal evaluation, and will participation commitments become contractual obligations? | Volume V Contract Documentation

A) The Government will evaluate Small Business Participation in accordance with the solicitation's evaluation criteria and proposal instructions.

The Small Business Participation Commitment Document submitted with the proposal may be incorporated into the contract and used as the basis for monitoring participation commitments during contract performance. Offerors should ensure that proposed participation commitments are realistic, achievable, and supported by their proposed teaming approach.

Q14.5 – Replacement of proposed subcontractors - If a proposed small business subcontractor becomes unavailable after award, may the contractor substitute another subcontractor? | Volume V Contract Documentation

A) Yes. The contractor may propose replacement subcontractors during contract performance, subject to any applicable contract requirements and Government review.

Any proposed substitution should maintain the contractor's ability to satisfy its Small Business Participation commitments and contract requirements. The contractor shall coordinate any significant changes in participation commitments with the Contracting Officer.

Q14.6 – Experience of proposed small business subcontractors - May offerors rely upon the experience and capabilities of proposed small business subcontractors as part of their overall team qualifications? | Volume II; Volume III

A) Yes. Offerors may describe the experience, qualifications, and capabilities of proposed subcontractors as part of their overall team approach where permitted by the solicitation.

The Government will evaluate experience, capabilities, and past performance in accordance with the solicitation's stated evaluation criteria.