Amendment 5
Selective Service System Website Modernization
Additional Frequently Asked Questions (FAQs)
June 26, 2026

The following questions and answers provide additional clarification regarding the Solicitation for Website Modernization Services. These FAQs supplement, but do not replace, the solicitation and previously issued amendments. Offerors should also refer to Amendment 3, which contains comprehensive responses to 120 vendor-generated questions spanning 47 pages. Together, Amendment 3 and this supplemental FAQ document provide the Government's official clarifications to assist offerors in preparing their proposals.

Project Schedule & Implementation

Q1. Project Schedule

Q) The solicitation anticipates substantial completion by September 25, 2026. Could the Government clarify whether all functionality is expected to be fully operational by that date, or whether "cutover ready" includes completion of development, testing, and deployment readiness with certain post-deployment activities continuing afterward?

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.

Existing Website Environment & Content Migration

Q2. Existing Website Environment

Q) Could the Government provide additional information regarding the current environment, including:

- Current Content Management System (CMS)
- Hosting platform
- Approximate number of webpages
- Number of documents and media assets
- Existing integrations with internal or external systems

A) Following award, SSS will provide available Government-furnished information necessary to support implementation, including, as available and applicable:

- Existing website content and content inventories
- CMS and application documentation
- Technical architecture and system documentation
- Interface specifications and integration documentation
- Available branding and design guidance
- Security and authorization documentation

SSS has not established a definitive inventory of website pages, documents, media assets, integrations, or technical artifacts for proposal purposes. Offerors should assume discovery, assessment, content analysis, and migration planning activities will be required as part of implementation.

The solicitation does not prescribe a specific CMS, hosting platform, or integration architecture. Offerors may propose solutions that satisfy the solicitation requirements. Detailed technical information regarding existing systems, interfaces, hosting, integrations, content inventories, and Government-furnished information will be coordinated with the successful Contractor following award.

Q3. Content Migration

Q) Could the Government provide an approximate inventory of:

- Existing webpages
- PDF and document files
- Images and media assets
- Existing forms or interactive components
- Legacy applications, if any, requiring migration or replacement

A) SSS has not established a definitive inventory of existing webpages, PDF and document files, images, media assets, forms, interactive components, or legacy applications for proposal purposes.

Offerors should assume that discovery, content inventory, content analysis, and migration planning activities will be required as part of the website modernization effort. Following award, SSS will provide available Government-furnished information, including existing content, technical documentation, application information, interface documentation, migration-related materials, and other relevant information, as appropriate.

The modernization effort is focused on the public-facing website and supporting content management capabilities. Existing SSS mission applications and business systems, including registration-related systems, remain the authoritative systems of record and are not being replaced under this solicitation. Where required, the

Contractor shall integrate the modernized website with existing Government-managed systems and services in accordance with the solicitation requirements. Offerors may identify reasonable assumptions regarding content volume, migration complexity, and legacy integration activities within their proposals.

System Integration

Q4. Automatic Registration Integration

Q) Could the Government provide additional information regarding the required integrations supporting Automatic Registration, including the number of systems involved, available APIs, interface specifications, and the availability of a testing environment?

A) SSS has identified five Government-managed integration endpoints that support the modernized website and related mission capabilities, including the Automatic Registration application. Detailed interface specifications, technical documentation, supported integration methods, endpoint ownership, available test environments, and contractor responsibilities will be provided to the successful Contractor following award, as appropriate.

Offerors should assume that integration may involve APIs, embedded services, iFrames, or other Government-approved mechanisms, as required by the solicitation. The Contractor is not expected to develop or replace the Automatic Registration application or associated business logic. Existing SSS mission systems will remain the authoritative systems of record, and the Contractor's responsibility is to securely integrate the modernized website with those Government-managed services.

SSS will provide available interface documentation, testing resources, and other Government-furnished information necessary to support integration activities following award. Offerors should identify any assumptions regarding integration requirements, interface documentation, testing environments, or Government-furnished information within their proposals.

Operations & Sustainment

Q5. Operations and Sustainment

Q) For pricing purposes, could the Government clarify the anticipated level of effort during the Operations and Sustainment period, including expected support hours, service level expectations, monitoring requirements, and anticipated enhancement requests?

A) SSS has not established a prescribed level of effort, staffing model, labor-hour estimate, or anticipated volume of Operations and Sustainment activities for proposal purposes. Offerors shall propose an Operations and Sustainment approach that supports the functional, security, accessibility, availability, performance, maintenance, monitoring, and operational requirements identified in the solicitation.

The Operations and Sustainment period is intended to support the continued operation, maintenance, security, monitoring, troubleshooting, patch management, content management support, defect resolution, and routine enhancements of the modernized website following implementation. Offerors should propose appropriate staffing, service levels, monitoring capabilities, maintenance processes, and operational support necessary to meet the solicitation requirements.

SSS has not established estimated quantities for support requests, enhancement requests, service desk activities, incident volumes, or operational workload. Offerors should independently determine the resources necessary to support their proposed solution and clearly identify any assumptions regarding support hours, service levels, monitoring requirements, maintenance activities, or anticipated enhancement effort within their proposals.

Development, Testing & Deployment

Q6. Development and Testing Environments

Q) Is the Contractor expected to design, provision, and manage the Development, Test, User Acceptance Testing (UAT), and Production environments, or will any of these environments be provided by the Government?

A) The Contractor shall be responsible for designing, provisioning, configuring, securing, operating, and maintaining the environments necessary to support successful implementation and operation of the contractor-provided solution, consistent with the solicitation requirements.

For proposal purposes, SSS requires Production and Staging environments. Offerors may propose additional non-production environments, such as Development, Test, User Acceptance Testing (UAT), training, demonstration, or sandbox environments, if they determine such environments are necessary to support their implementation, testing, security, deployment, training, or operational approach.

SSS will provide available Government-furnished information, interfaces, testing resources, and access to Government-managed systems necessary to support integration and acceptance testing, as appropriate. The specific configuration, access requirements, responsibilities, and use of Government and contractor-managed environments will be refined and coordinated with the successful Contractor following award. Offerors should clearly identify any assumptions regarding environment architecture, provisioning, management responsibilities, and Government-furnished resources within their proposals.

Q7. Government Review Process

Q) Could the Government provide an overview of the anticipated review and approval timelines for design deliverables, testing, security documentation, and production deployment? This information would assist offerors in developing realistic project schedules and resource plans.

A) SSS will make reasonable efforts to review and provide feedback on project deliverables in a timely manner throughout contract performance. For proposal purposes, SSS has not established mandatory review or approval turnaround times for design deliverables, testing, security documentation, AI governance submissions, user acceptance testing, production deployment, or other project deliverables.

Offerors should propose a realistic project schedule that includes adequate time for SSS review, comments, revisions, testing, security and privacy activities, deployment preparation, and approval processes. The proposed schedule should account for

iterative collaboration between SSS and the Contractor throughout discovery, design, development, testing, security authorization, and deployment.

Following award, SSS and the successful Contractor will collaboratively establish detailed project schedules, review procedures, milestone dates, deliverable expectations, communication protocols, and governance processes to support successful execution of the modernization effort. Offerors should clearly identify any assumptions regarding SSS review activities, approval dependencies, or schedule impacts within their proposals.

Industry Engagement

Q8. Industry Day / Information Session

Q) Does the Government anticipate holding an Industry Day, technical briefing, vendor question-and-answer session, or any other informational meeting where prospective offerors may gain a better understanding of the project requirements? If so, we would appreciate information on how to participate.

A) SSS will consider conducting a technical briefing or vendor question-and-answer session during the solicitation review process. If such an event is scheduled, SSS will provide appropriate notification to all prospective offerors through an official solicitation amendment or other authorized procurement communication.

Q9. Project Plan and Schedule Submission

Q) PWS 7.1 states the Initial Draft Project Plan and Comprehensive Project Timeline are due by the RFP close date. Please confirm these are submitted within Volume II as part of Factor 1 and whether they count toward the 80-page limitation.

A) Yes. The Initial Draft Project Plan and Comprehensive Project Timeline shall be submitted as part of Volume II (Technical Proposal). These required submissions are excluded from, and will not be counted toward, the 80-page limitation applicable to Volume II.

Q10. Hosting Environment During Contract Performance

Q) PWS Part 5.5 requires migration from the Contractor-hosted cloud to the Agency-selected cloud environment during transition-out. Please clarify whether the production environment is expected to remain contractor-hosted during the base period and option years, or whether SSS expects migration to an Agency-owned Azure environment before or during the period of performance.

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, documentation, configurations, integrations, and related materials to a Government-designated environment or successor contractor at the conclusion of contract performance.

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

Q11. Personnel Screening and Suitability Requirements

Q) The technical proposal instructions reference appropriately experienced and cleared personnel. Please clarify whether contractor personnel require security clearances, public trust determinations, U.S. citizenship, background investigations, or other suitability requirements.

A) SSS expects contractors to have completed appropriate personnel background investigations and suitability screening for personnel assigned to perform work under the contract.

Contractor personnel requiring access to Government systems, facilities, information, or resources may be subject to additional Government suitability determinations, access requirements, or background investigation requirements, as applicable. SSS will coordinate any specific access, onboarding, identity verification, or suitability requirements with the successful Contractor following award.

Offerors should ensure that personnel assigned to the contract are appropriately screened and suitable to perform the required work.

Q12. Disaster Recovery Objectives

Q) Please provide the current Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for the website, CMS, backend database, integrations, and public-facing registration workflows. If these are not currently defined, please provide the Government's target recovery objectives for the proposed solution.

A) The Contractor shall provide documented incident resolution status updates at Government-defined intervals until closure of the incident.

Severity – Minimum response and remediation timelines shall be:	**Response Time**	**Restoration / Mitigation**
Critical (production outage/security compromise)	1 hour	4 hours
High (major functionality degradation)	2 hours	24 hours
Moderate (partial service degradation)	4 business hours	5 business days
Low (minor defects/cosmetic issues)	2 business days	Government-approved schedule

---

Q13. Government Review Cycle

Q) Please clarify the expected Government review and approval cycle for design deliverables, testing artifacts, security documentation, and deployment readiness.

A) The Government will make reasonable efforts to review and provide feedback on wireframes, mockups, design specifications, content decisions, User Acceptance Testing (UAT) findings, security artifacts, deployment readiness documentation, and other required deliverables in a timely manner consistent with the approved project

schedule. Specific review and approval timeframes will be established after award and coordinated between the Government and the successful Contractor.

Q14. OMB M-22-18 Software Attestation

Q) Please clarify the software attestation documentation required to comply with OMB Memorandum M-22-18.

A) Offerors shall comply with applicable Federal software security requirements, including OMB Memorandum M-22-18 and other applicable Federal cybersecurity requirements.

The Government is not prescribing specific software security artifacts (such as SSDF mappings, SBOMs, code scanning results, supplier attestations, or software provenance documentation) as part of the proposal submission. However, the successful Contractor may be required to provide documentation necessary to support security reviews, compliance verification, and system authorization activities.

Q15. Government Security Assessments

Q) Please clarify the Government's expectations regarding security assessments, penetration testing, remediation, and authorization activities.

A) The successful Contractor shall support Government-directed security assessments, penetration testing, vulnerability assessments, and authorization activities, as required. The timing, scope, testing environment, reporting process, remediation timelines, retesting procedures, and acceptance criteria will be coordinated following award as part of the Government's security assessment and authorization process.

Q16. CMS User Roles

Q) Please identify the expected CMS/backend user roles, permission levels, approval workflows, and role mappings.

A) The Government has not prescribed specific CMS user roles, permission levels, approval workflows, publishing roles, or role-to-group mappings for proposal purposes.

Offerors shall propose a CMS governance model that supports role-based access control, separation of duties, configurable approval workflows, auditing, and secure content management consistent with the solicitation requirements.

The proposed solution shall integrate with Microsoft Entra ID (formerly Azure Active Directory) for Government user authentication and authorization. Specific user roles, group mappings, and workflow configurations will be finalized during implementation in coordination with the Government.

Q17. CMS Backend Portal Access

Q) 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.

Q.18 Log.gov Is Not Required

Q) Amendment 0002 states that SSS does not currently maintain a Login.gov agreement and that offerors may propose secure authentication and identity-proofing solutions that meet applicable federal security and privacy requirements. Please clarify whether public registrants/end users must authenticate through the contractor-provided website or only through existing registration services and identify the required identity assurance/authenticator assurance level and any acceptable identity-proofing providers or 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**.**

Q19 Plan to Monitor User Access

Q) 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.

Q20. Content Approval Workflows

Q) Please clarify the required content review and approval workflow within the CMS.

A) The CMS shall support configurable draft, review, approval, scheduled publishing, and content management workflows. The Government has not prescribed mandatory approval chains or specific review participants. Depending on the nature of the content, reviews may involve program offices, public affairs, legal counsel, security personnel, or other designated Government stakeholders. Final workflow requirements will be established during implementation.

Q21. Multilingual Content

Q) Does the Government require multilingual content or translation capabilities?

A) The Government does not currently require multilingual content, translation workflows, or language toggle functionality. However, the proposed solution should be capable of supporting future multilingual content requirements, if needed, and shall comply with all applicable Federal accessibility requirements.

Q22. CMS Content Model

Q) Please identify the required CMS content types, templates, reusable components, metadata, taxonomy, and search indexing requirements.

A) The Government has not prescribed specific CMS content types, templates, reusable components, navigation structures, metadata fields, taxonomy, SEO fields, document libraries, media libraries, or search indexing rules for proposal purposes.

Offerors shall propose a scalable content management architecture that supports the solicitation's functional, accessibility, usability, security, search, and governance requirements. Detailed information architecture and content models will be refined collaboratively during implementation.

Q23. Automatic Registration Application

Q) Is the Contractor responsible for developing the Automatic Registration application?

A) The Contractor is not required to develop or replace the Automatic Registration application. The Contractor shall ensure that the modernized website supports secure integration with existing and future Government-managed Automatic Registration capabilities in accordance with the solicitation requirements.

Q24. API Documentation

Q) Will the Government provide interface specifications, API documentation, and testing resources?

A) Following contract award, the Government anticipates providing available interface specifications, API documentation, test credentials, staging environments, system access, technical documentation, and Government-furnished information necessary to support required integrations, as applicable. Specific interface dependencies, access requirements, and delivery schedules will be coordinated with the successful Contractor during implementation.

Q25. Analytics

Q) Please clarify the required analytics implementation.

A) The Government has not prescribed a specific analytics platform, dashboard configuration, or reporting solution for proposal purposes. Offerors shall propose an analytics approach that complies with applicable Federal privacy, accessibility, and security requirements while supporting measurement of website usage, user engagement, and operational performance. Final reporting requirements will be established during implementation.

Q26. Contract Specialist Email Address

Q) Attachment 2 identifies a different Contract Specialist email address than the solicitation instructions. Please confirm the correct email address for proposal submissions, questions, and Past Performance Questionnaire (PPQ) correspondence.

A) The correct Contract Specialist email address is the email address identified in the official solicitation for proposal submissions and communications. Offerors should rely on the contact information contained in the most current solicitation amendment. If inconsistencies exist between solicitation attachments, the contact information provided in the solicitation instructions and subsequent amendments governs.

Q27. Proposal Email Size Limitation

Q) Please clarify whether the 35 MB email limitation applies per email transmission or to the entire proposal submission.

A) The 35 MB limitation applies to each individual email transmission. Offerors may submit proposal volumes across multiple emails if necessary to accommodate file size limitations. Offerors anticipating submission issues should coordinate with the Contracting Officer before the proposal due date.

Q28. Long-Term Mission Outcomes

Q) Beyond modernizing the technical platform itself, what are the Government's most important mission outcomes for this effort over the next several years?

A) The Government's desired outcomes are reflected throughout the solicitation requirements, performance objectives, and evaluation criteria. Offerors should develop their proposed solutions based upon those stated requirements. No additional mission objectives are being provided through this question-and-answer process.

Q29. Surge Readiness

Q) Has the Government established specific surge user or contingency activation requirements that offerors should consider?

A) The Government has not established specific surge user volumes or contingency activation requirements for proposal purposes. Offerors should propose solutions that incorporate appropriate scalability, resiliency, availability, and continuity-of-operations capabilities consistent with the solicitation requirements.

Q30. Authority to Operate (ATO)

Q) Will the Contractor inherit an existing Authority to Operate (ATO), or will a new ATO be required?

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 completion of required ATO-related activities.

Q31. Content Governance

Q) Does the Government have an existing content governance and approval workflow the Contractor should preserve or improve?

A) The Government maintains existing content review and approval processes. Offerors should propose a content governance model that supports efficient content management while accommodating Government review and approval responsibilities. Final governance processes will be established collaboratively during implementation.

Q32. Base and Option Period Dates

Q) Please clarify the intended period of performance for the Base Period and Option Years.

A) CLINs 0001 through 0003 comprise the Base Period and cover implementation and initial operations activities beginning upon contract award. For pricing purposes, offerors should assume the Base Period extends from contract award through September 25, 2026.

CLIN 1001 (Option Year 1) begins September 26, 2026, and continues through September 25, 2027. Subsequent option periods follow annually thereafter.

Q33. AI Chatbot Security Requirements

Q) For the AI-enabled conversational capability, does the Government require the chatbot product itself to possess a separate FedRAMP authorization?

A) The proposed AI-enabled conversational capability shall comply with all applicable Federal security, privacy, and authorization requirements. The Government does not require the chatbot product itself to possess a separate standalone FedRAMP authorization, provided the overall solution satisfies applicable Federal security requirements and operates within an appropriately authorized environment.

Q34. Automatic Registration Application

Q) Is the Automatic Registration application Government-furnished, and who is responsible for its development?

A) The Automatic Registration application is Government-managed. The Contractor is responsible for integrating the modernized website with the application in accordance with the solicitation requirements. Available interface documentation and integration information will be provided following contract award, as appropriate.

Q35. Government Authority to Operate Approval

Q) Will the Government serve as the Authorizing Official for issuance of the Authority to Operate (ATO)?

A) The Government will serve as the Authorizing Official for issuance of the Authority to Operate (ATO). Authorization schedules will be coordinated following award based upon project progress, submission of required security documentation, completion of security assessments, and applicable Government review processes.

Q36. Authentication Architecture

Q) Would the Government accept an architecture utilizing Microsoft Entra ID for Government users and login.gov for future public-user authentication?

A) Yes. Offerors may propose an architecture utilizing Microsoft Entra ID for Government administrative users and login.gov, or another Government-approved identity solution, for future public-user authentication, provided the proposed solution satisfies all applicable Federal identity, security, and privacy requirements.

Q37. Website Availability Measurement

Q) Will planned maintenance or outages caused by Government-managed external systems be excluded from uptime calculations?

A) Planned maintenance coordinated with the Government will not be considered service downtime. Downtime attributable solely to Government-managed external systems outside the Contractor's operational control will be evaluated consistent with the terms of the contract. Offerors may propose appropriate monitoring approaches, including synthetic monitoring, real-user monitoring, or comparable industry-standard capabilities.

Q38. Future Enhancements

Q) Are there any pending major enhancements or new feature requests beyond those identified in the solicitation?

A) The Government has not identified additional major enhancement requirements beyond those described in the solicitation. Offerors should base their proposed solutions on the requirements contained within the solicitation.

Q39. Government-Furnished Creative Assets

Q) Will the Government provide branding assets, photographs, and other creative content?

A) The Government will provide available branding guidance, content, photographs, logos, and other Government-owned creative assets necessary to support implementation. Offerors may propose additional creative services as part of their overall solution, if appropriate.

Q40. Discovery Phase Stakeholders

Q) Approximately how many Government stakeholders should offerors expect to participate during Discovery?

A) Offerors should assume participation from both business and technical stakeholders throughout discovery and implementation. Government participants may include executive leadership, communications personnel, program offices, information technology, cybersecurity, and other subject matter experts, as appropriate.

Q41. Schedule Flexibility

Q) Will the Government consider schedule adjustments if delays occur due to Government dependencies?

A) The Government recognizes that schedule impacts may occur due to Government review activities or unforeseen circumstances. If Government-caused delays materially affect project execution, schedule adjustments may be considered through appropriate contract administration processes.

Q42. Contractor-Managed FedRAMP Environments

Q) Are contractor-managed FedRAMP-authorized cloud environments acceptable?

A) Yes. Contractor-managed FedRAMP-authorized environments are acceptable provided they satisfy all applicable solicitation, Federal security, and hosting requirements.

Q43. On-Site Support

Q) Is on-site support required during contract performance?

A) Performance under this contract is expected to be primarily remote. Limited on-site support at SSS Headquarters may occasionally be required, as coordinated with the Government.

Q44. Best Value Tradeoff

Q) May a higher-rated technical proposal be selected at a higher price under the solicitation's best-value tradeoff methodology?

A) Yes. Contract award will be made in accordance with the solicitation's stated best-value tradeoff methodology. A higher-rated technical proposal may be selected if the Government determines that the additional value justifies any associated price premium consistent with the evaluation criteria.

Q45. Government Subject Matter Expert Support

Q) Will the Government provide subject matter experts and content owners to support website content development and review?

A) Yes. The Government will provide appropriate subject matter experts and designated content owners to support content development, review, and approval activities throughout contract performance.

Q46. Design Standards

Q) Are there preferred Government design systems, branding standards, or style guides that should be incorporated into the proposed solution?

A) Yes. The Government will provide applicable branding guidance, style standards, and design preferences during implementation. Offerors should also consider applicable U.S. Web Design System (USWDS), Digital.gov guidance, and Federal accessibility requirements when developing their proposed solution.

Q47. Risk Management Framework (RMF) Documentation

Q) Is the Contractor expected to develop a complete ATO package or only provide RMF artifacts necessary for Government authorization?

A) The successful Contractor shall provide the security documentation, Risk Management Framework (RMF) artifacts, testing support, and other materials reasonably necessary for the Government to complete the authorization process and issue an Authority to Operate.

Q48. Third-Party SaaS Services

Q) May FedRAMP-authorized third-party SaaS services be utilized for capabilities such as search, analytics, chatbot functionality, workflow automation, or accessibility monitoring?

A) Yes. FedRAMP-authorized third-party SaaS services may be proposed where appropriate, provided they are compatible with Microsoft Azure Government, satisfy all applicable Federal security requirements, and support the solicitation objectives.

Q49. Azure Government Hosting

Q) Does the Microsoft Azure Government hosting requirement apply to all components of the proposed solution?

A) The primary hosting environment shall utilize Microsoft Azure Government. Supporting components, including content management, analytics, search, workflow, chatbot, and related services, may utilize compatible technologies provided they fully integrate with the Azure Government environment and satisfy all applicable Federal security and hosting requirements.

Q50. Website Content Disposition Baseline Provided at Award

Q) Will the Government provide a content disposition baseline at award showing which existing sss.gov elements (State Director directories, Classification Status Forms, Registration Verification interfaces, and similar content) are being retired in favor of the Automatic Registration application, retained in the modernized website, or deferred to a later phase?

A) Yes. Following contract award, the Government will provide the successful Contractor with a content disposition baseline identifying, to the extent available, which existing sss.gov content and functionality will be retained, modernized, retired, or otherwise addressed as part of the implementation effort. The Government anticipates that much of the existing website content will remain and be modernized, including the Registration Verification page, Change Registration Information

functionality, Classification Status Forms, and other public-facing informational content.

The content disposition baseline will be refined during the discovery phase in coordination with the successful Contractor as part of the overall content inventory and migration planning process.

Q.51. Website Uptime Measurement Methodologies

Q) PWS 2.7 requires 99.9% uptime and PWS 8.1 specifies 99.9% uptime measured monthly. Please confirm the exact SLA measurement methodology, exclusions, maintenance windows, reporting requirements, required page-load/Core Web Vitals/response-time/RTO/RPO/error-rate thresholds, and whether uptime/performance applies only to the public website or also to the CMS, staging environment, chatbot, and integrated registration workflows.

A) The uptime and performance requirements for this effort are those identified in the solicitation. SSS has not established additional service-level metrics, measurement methodologies, exclusions, maintenance windows, response-time thresholds, recovery objectives, error-rate thresholds, Core Web Vitals requirements, or reporting requirements beyond those specified in the solicitation. Offerors should describe their proposed approach for monitoring, measuring, reporting, and achieving the required service levels.

Q52. iFrame Embedding Requirement

Q) For the iframe embedding requirement, will the external registration application share the sss.gov root domain or run from a separate FQDN, and is the Contractor expected to set the Content Security Policy, CORS, and frame-ancestors directives governing that relationship?

A) The external registration application will share the sss.gov root domain but will operate under a separate subdomain. The Contractor shall implement and maintain the appropriate application-level security configurations for all solution components

under its control, including Content Security Policy (CSP), Cross-Origin Resource Sharing (CORS), *frame-ancestors*, and other applicable security controls, consistent with least-privilege principles and subject to Government security review and approval.