Request for Proposal

Website and Digital Platform Design, Development, Hosting, and Maintenance for Project Constellation

1. Statement of Purpose

Meridian seeks an experienced firm to design, develop, launch, set up hosting server, and support the maintenance of a public website and secure member platform for Project Constellation – at least for the duration of the performance period (Sept. 30, 2028). The complementary systems will increase public awareness of U.S. space leadership while supporting ongoing engagement, knowledge exchange, capacity building, and partnership development among approved participants.

2. Background Information

Meridian International Center is a nonpartisan center for diplomacy founded in 1960 and headquartered on a historic campus in Washington, D.C. Our mission is to empower the next era of leaders to advance diplomacy for a better future. Our programs strengthen American leadership by accelerating collaboration on shared challenges, increasing economic competitiveness, and building geopolitical resilience. We equip leaders from government, business, science and technology, cities and states, culture and sports with the insights, networks, and resources to navigate a complex world.

Meridian is seeking an experienced web development firm to design, launch, and maintain a public website with a public front-end and an authenticated, a secure, password-protected member-only platform for Project Constellation. Project Constellation is a year-round U.S. Government initiative that connects emerging space nations with U.S. policy, technical, and commercial expertise to advance American leadership, economic opportunity, and responsible

Because the member platform will hold personal and organizational information about international participants, including foreign government officials, and will be funded through a U.S. Department of State award, Meridian treats security, privacy, and data protection as core requirements of this procurement rather than secondary considerations.

The selected vendor will design, launch, host, and maintain both systems. Meridian will dedicate staff resources for continuous content management and routine platform administration.

3. Scope of Work

Meridian seeks a vendor to design, build, launch, and maintain the website, consisting of these components:

A. Public Website

The Project Constellation website will be the initiative's public-facing digital hub and primary public diplomacy tool. It will increase awareness of U.S. leadership in the global space sector and provide a visible entry point into the Project Constellation network. The website must include:

- A public events calendar
- Information on partnership, training, and exchange opportunities
- NASA and other U.S. Government resources
- Partnership spotlights and country success stories
- Commercial and academic engagement opportunities
- Participant success stories and regularly updated content highlighting innovation, collaboration, and responsible space development
- Multimedia content, including short videos, podcasts, and State of Global Space infographics (to be provided)
- A contact and interest form protected against spam and automated abuse
- A clear pathway from the public website to the member platform
- Search engine optimization and social media integration to support Meridian's targeted digital outreach campaign

B. Secure Member Platform

A password-protected platform, accessible only to approved members, will give governments, industry representatives, academics, entrepreneurs, and other stakeholders from participating countries exclusive access to a trusted U.S.-supported international network. The platform must include:

- Participant profiles and a searchable member directory, with member-controlled visibility settings for personal contact details
- A curated resource library highlighting U.S. Government tools, policies, and technical resources
- An archive of webinars and virtual programming
- A listserv sign up
- Communications toolkits that facilitate ongoing interaction among Meridian, U.S. embassies, U.S. companies, universities, technical experts, and international participants
- A dedicated request portal through which members can seek technical assistance, propose follow-on engagements, identify training needs, request connections to U.S. partners, or express interest in future delegations and exchanges, with secure handling of any file uploads. Meridian would need a moderator role and the capacity to pre-approve posts

- A partnership opportunity database that captures both international needs and U.S. capabilities; supports matchmaking among governments, universities, companies, investors, and technical experts; tracks emerging partnership opportunities; and documents collaboration outcomes over time. Meridian would need a moderator role and the capacity to approve posts.

- Monitoring, evaluation, and learning functionality that tracks user engagement, resource utilization, partnership leads, technical assistance requests, training participation, and follow-up outcomes, and provides real-time, exportable reporting on program performance, with export rights limited to authorized roles and all exports logged

C. Technical and Functional Requirements

- Fully functional and fast, with a full page load time of 2 seconds or less for key public pages, measured on a standard broadband connection and on a mid-range mobile device over a 4G connection using a tool agreed with Meridian
- Compatible with the current and previous major versions of Chrome, Firefox, Edge, and Safari, including mobile Safari and Chrome on iOS and Android
- Fully mobile-friendly, with responsive design based on screen size, platform, and orientation
- Accessible in conformance with Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, verified by both automated and manual testing
- Ability for Meridian editors and administrators to easily search for, draft, edit, preview/QA, schedule, publish, and update content through an editorial workflow, rather than a code deployment
- Ability for editors and administrators to easily search, navigate, and restore previous versions of content, with tracking of users, timestamps, and indications of what changed
- Ability for administrators to manage end-user accounts (for example, approve members, reset passwords, and deactivate or delete users)
- Analytics and reporting tools that allow administrators to view and export engagement and performance data, configured to respect visitor privacy and cookie consent requirements
- Ability to pull and render specific data and content from linked databases, preferably automatically
- Ability to integrate securely with third-party tools as needed (for example, video and webinar hosting, email and listserv services, and social media)
- Vendors may propose any technology or platform that meets these requirements; equivalent solutions are welcome. Proposals must name the content management system, hosting provider, and any third-party components, and must confirm that every component will remain under active vendor support for the full period of performance

D. Security, Privacy, and Data Protection Requirements

Vendors must address each item below in their proposal and complete the response checklist in Appendix A.

D.1 Identity and Access Management

- Multi-factor authentication (MFA) is required for all administrator, editor, and vendor accounts, and must be available to members
- Single sign-on (SSO) for Meridian staff through Meridian's Microsoft Entra ID tenant, so that staff access is granted and removed through Meridian's existing account processes
- Password, account lockout, and session timeout rules consistent with NIST Special Publication 800-63B
- Defined roles with least-privilege permissions, at minimum: public visitor, member, member group (for example by country or sector, if needed), content editor, platform administrator, and vendor support. Vendors must provide a role and permission matrix
- A documented membership approval workflow, including the vetting steps Meridian will perform, an audit trail of approvals and denials, and automatic expiry or periodic review of inactive accounts
- Vendor access to production systems must use named individual accounts with MFA, be logged, and be revocable by Meridian at any time. Shared or generic administrator accounts are not permitted
- Meridian will retain owner-level administrative access to all hosting, domain, DNS, content management, and third-party service accounts throughout the period of performance

D.2 Data Protection and Privacy

- Vendors must provide an inventory of the personal and organizational data the systems will collect, where it is stored, and who can access it
- All data must be encrypted in transit using TLS 1.2 or higher with HTTP Strict Transport Security (HSTS), and encrypted at rest, including backups
- Member, contact, and request data must be hosted in the United States unless Meridian approves otherwise in writing
- The systems must support compliance with applicable privacy laws for an international audience, including the EU General Data Protection Regulation where it applies. This includes a privacy notice, consent and cookie management, and the ability to fulfill requests to access, correct, export, or delete a person's data
- Vendors must propose data retention and deletion rules for member, request, and analytics data, for Meridian approval
- Vendors must list all subcontractors and third-party services that will store or process Meridian data
- The selected vendor must sign Meridian's Data Processing Agreement, which will be provided to shortlisted vendors

D.3 Vendor Security and Governance

- Vendors must describe their own security program, including any certifications, and complete a Meridian vendor security assessment before contract award
- Personnel with access to production systems or Meridian data must have completed background checks and security awareness training
- Vendors must disclose any development, support, or hosting performed outside the United States, and any subcontractors
- The selected vendor must carry cyber liability insurance in an amount to be set in the contract
- The vendor will comply with Meridian's information security policies as they apply to the systems, and will coordinate with Meridian IT on access controls and security changes

E. Contractor and Meridian Responsibilities

- Organize and present information in a visually compelling way that best serves key audiences, with unifying themes, fonts, color, layout, and branding
- Provide both strategic assistance and tactical service while designing, launching, and maintaining both systems
- Perform strategic analysis and design of back-end and front-end system architecture
- Provide hosting, uptime monitoring, ongoing technical maintenance, security updates, backups, and responsive technical support so that both systems remain active, valuable, and responsive throughout the period of performance
- Provide a responsibility matrix showing which security and operational tasks are performed by the vendor, the hosting provider, and Meridian
- Train Meridian staff responsible for content management and platform administration, including secure administration practices, and provide user and administrator documentation
- Provide a transition plan at the end of the period of performance or on request, including export of all content and data in standard, non-proprietary formats, transfer of all accounts and credentials to Meridian, and written certification of data deletion from vendor systems

Meridian will dedicate staff resources to continuous content management and routine platform administration, while the contractor will provide the technical systems, training, maintenance, security, and support described above.

4. Outcome and Performance Standards

The delivered systems must meet the requirements in Section 3, including the performance, browser compatibility, responsive design, accessibility, language support, and security, privacy, and data protection requirements.

Each stage will be accepted only after the vendor documents functional, accessibility, performance, and security testing and resolves all critical and high-severity defects and security findings. Security test results are a condition of acceptance for each stage.

Vendors must propose service levels covering at minimum: availability of 99.9% monthly uptime, excluding scheduled maintenance agreed with Meridian; maintenance coverage (support hours and days); incident response and resolution times by severity; escalation procedures; patching timelines; and corrective-action processes. Final service levels, service credits, and remedies will be agreed in the contract.

5. Deliverables

This project will be completed in three stages. Final milestones and dates will be set at contract signing and aligned with the Project Constellation workplan.

- **Stage 1: Core Public Website** (deadline: January 15, 2027). Rapid launch of the basic public website, to be completed no later than the second full week of January 2027. Stage 1 includes the design framework and branding, a homepage and project overview, a public events calendar, information on partnership, training, and exchange opportunities, links to NASA and other U.S. Government resources, and a protected contact and interest form. It must be mobile-friendly, accessible, and secure, with MFA for all administrator and editor accounts, a completed baseline security review, and an editorial workflow that Meridian staff can use immediately.
- **Stage 2: Advanced Public Website Features** (target: mid-March 2027). Expansion of the public website with multimedia content (short videos, podcasts, partnership spotlights, country success stories, and State of Global Space infographics), participant success stories, commercial and academic engagement opportunities, search engine optimization and social media integration, and a clear pathway to the member platform.
- **Stage 3: Private Member Platform** (target: April 2027). Design, build, and launch of the secure, password-protected member platform with all of the features described in Section 3.B, following a completed independent penetration test and remediation of critical and high-severity findings. Meridian asks that Stage 3 be completed at least one month before the 2027 U.S. Space Forum (scheduled for June 2027 in Vienna), ideally by April 2027.

Across all stages, the vendor will be expected to provide the following:

- Discovery and requirements: a kickoff meeting, consultation with Meridian staff (including Meridian IT), and a requirements and site-architecture document that includes a data flow diagram and a security architecture overview
- Design: wireframes and visual design mockups for the public website and the member platform, for Meridian approval

- Development and testing: a fully functional build of each stage, including content loading and quality assurance, accessibility, security, and performance testing, with written test results
- Launch: staged launches of the public website (Stages 1 and 2) and the member platform (Stage 3), with launch support
- Training and documentation: administrator and content-manager training sessions and written documentation, including an administrator security guide
- Security documentation: role and permission matrix, data inventory, incident response plan, backup and recovery plan, software bill of materials, and penetration test summary
- Hosting and maintenance: ongoing hosting, technical maintenance, security patching, and support for both systems throughout the period of performance (anticipated to be two years)
- Reporting: regular status updates during development; and during operation, monthly reports covering uptime, support tickets, patching status, security events, and platform analytics

Vendors should propose a detailed timeline that meets the Stage 1 deadline of January 15, 2027, the Stage 2 target of mid-March 2027, and the Stage 3 target of April 2027. Because Stage 1 is time-sensitive, Meridian anticipates a rapid vendor selection and contract execution, with design work beginning promptly afterward.

6. Payments and Pricing

The proposal should include a detailed cost proposal that separates: (a) one-time design, development, and launch costs, itemized for each of the three stages; (b) the annual hosting, maintenance, security, and technical support fee for each year of the anticipated two-year period of performance; (c) security testing costs, including the pre-launch and annual penetration tests; (d) pricing for an optional extension beyond the two-year period; and (e) any optional enhancements, priced separately.

- Meridian encourages vendors to propose a firm fixed-price contract. If proposing time and materials, please provide hourly rates by staff level, the resources and number of each needed for this project, estimated hours by stage, and a not-to-exceed ceiling amount.
- Proposals should be all-inclusive of expenses. Any third-party licenses, hosting, security tools, or other recurring costs must be itemized.
- Domain name(s) must be registered in Meridian's name. Vendors should itemize domain registration, hosting, and renewal costs, and confirm that all domains, hosting accounts, source code, content, and data will be transferred to Meridian at the end of the period of performance or upon request.
- Vendors should state their key pricing assumptions (for example, number of pages, content volume, languages, and member accounts) and provide rates or unit pricing for

work beyond the stated scope. No out-of-scope work may begin without written approval from Meridian's designated representative.

- Meridian anticipates milestone-based payments tied to accepted deliverables. Vendors may propose an alternative payment schedule. Any service credits, remedies, or penalties for missed service levels will be negotiated in the final contract.

7. Contractual Terms and Conditions

The anticipated hosting, maintenance, and support period is two years, with an optional extension to be priced separately.

Meridian has been awarded the Project Constellation cooperative agreement by the U.S. Department of State. Work under this RFP will be funded through that award and is subject to applicable U.S. Department of State approvals and federal requirements, which will flow down to the selected vendor as required.

- Proposals must remain valid for a period not less than 90 days after the submission deadline.
- Meridian reserves the right to accept or reject any proposal, cancel the solicitation, and reject all proposals at any time prior to the award of the contract.
- The selected vendor will sign and adhere to Meridian's Data Processing Agreement and will comply with the prohibition on use of certain telecommunications and video surveillance services or equipment as defined in Section 889(a)(1) of the National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) and as more specifically defined in Federal Acquisition Regulation (FAR) clause 52.204-25, "Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment." Vendors must confirm compliance for all proposed hardware, software, and hosting components.
- Meridian's Terms and Conditions are incorporated by reference: https://meridian.vendorrisk.com/guest_document/35351/e211a777626c3
- Meridian and the vendor will not have any binding obligation to each other until a contract for services is signed by both parties. If a contract is signed, the relationship of the vendor to Meridian will be that of an independent contractor only. A W-9 tax and vendor form with banking details will be required to set up a contract for services.
- Vendors should identify any third-party licenses or proprietary components included in their proposed solution, along with any associated recurring costs.

8. Requirements for Proposal Preparation

Proposals should be submitted electronically in PDF format and should not exceed 20 pages, excluding appendices, the Appendix A response checklist, and work samples. Proposals must include the following information:

- Firm name and contact information

- A short narrative describing the history (including year founded) of the firm and its relevant expertise, including experience building secure membership platforms
- An explanation of how the firm would engage with Meridian, including proposed timeline for each stage, scope, and a basic wireframe
- A technical approach describing the proposed architecture, content management system, hosting provider, integrations, accessibility approach, and language support
- A security and privacy approach addressing every requirement in Section 3.D, plus the completed Appendix A checklist
- A maintenance and service-level plan addressing Section 4
- At least three (3) examples of similar work, which could include screenshots, images, and URLs
- A cost proposal as described in Section 6, including pricing assumptions, third-party costs, security testing costs, and pricing for an optional extension
- Any exceptions to this RFP or dependencies on Meridian

9. Evaluation and Award Process

Meridian will evaluate proposals on a best-value basis using the following criteria:

Criterion	Points
Technical approach: design, architecture, functionality, integrations, and timeline	30
Security, privacy, and accessibility approach	25
Cost and cost reasonableness	25
Past performance and relevant experience	20
Total	**100**

Procurement schedule: confirmation of interest by December 3, 2026; questions by December 4, 2026; **proposal submission by December 11, 2026, at 6:00 PM Eastern Time**; anticipated vendor selection by December 17, 2026. Meridian may request clarification, a demonstration, or additional due diligence, including a vendor security assessment, before award.

10. Contacts

Frank Justice | Vice President, Open Diplomacy Programs | Meridian International Center

Email: ProjectConstellation@meridian.org | Phone: 202-939-5583

Submit proposals to ProjectConstellation@meridian.org with subject line: "Project Constellation Website and Digital Platform RFP: [Vendor Name]." All questions must be submitted to the same address.

Appendix A: Security and Privacy Response Checklist

Please complete this checklist and include it with your proposal. For each item, indicate Yes, Partial, or No, and provide a brief explanation or reference to the relevant page of the proposal.

ID	Requirement	Section	Yes / Partial / No	Vendor explanation
S-01	MFA for administrator, editor, and vendor accounts; available to members	3.D.1		
S-02	SSO for Meridian staff through Microsoft Entra ID	3.D.1		
S-03	Password, lockout, and session rules per NIST SP 800-63B	3.D.1		
S-04	Role and permission matrix with least-privilege access	3.D.1		
S-05	Membership approval workflow with audit trail and account review	3.D.1		
S-06	Named, logged, revocable vendor access; no shared admin accounts	3.D.1		
S-07	Personal data inventory	3.D.2		
S-08	Encryption in transit (TLS 1.2+, HSTS) and at rest, including backups	3.D.2		
S-09	U.S. data hosting	3.D.2		
S-10	Privacy notice, consent and cookie management, data subject requests	3.D.2		
S-11	Data retention and deletion rules	3.D.2		
S-12	List of subcontractors and third-party processors	3.D.2		
S-13	Baseline security review before Stage 1; penetration test before Stage 3 and annually	5, 6		
S-14	Incident response plan	5		
S-15	Backup and recovery plan	5		
S-16	Background checks, security training, offshore disclosure, cyber insurance	3.D.3		
S-17	Section 889 / FAR 52.204-25 compliance for all components	7		
S-18	WCAG 2.1 AA and Section 508 conformance	3.C		