EURASIA FOUNDATION

Request for Proposals
Website Maintenance and Hosting

DETAILS

Job type: Contractor
Anticipated period of performance: June 1, 2024, onward (subject to contract renewals)
Application deadline: May 6, 2024

SUMMARY

Eurasia Foundation announces a competitive tender to maintain and host the organization's corporate website. The chosen strategic partner must be a firm that has at least five years of experience managing website design projects and that uses best practices regarding: research-based website design, UX and usability testing, information architecture, content strategy, search engine optimization, website development and deployment, website and web server security; and website hosting.

ABOUT EURASIA FOUNDATION

Eurasia Foundation is a nonprofit international development organization committed to the idea that societies function best when people take responsibility for their own civic and economic prosperity. We envision a future where all people have the opportunity to realize their potential and transform their societies. Since 1992, Eurasia Foundation has equipped forward-thinking people across Europe, Eurasia, Asia, the Middle East and North Africa with the tools, knowledge, and resources needed to address issues of concern in their communities. Our success showcases the power of a vibrant civil society to drive real and lasting change.

SCOPE OF WORK

The Vendor will complete the following tasks beginning on June 1, 2024:

Part I: Website Hosting

Host Eurasia Foundation's corporate website, www.eurasia.org. Website hosting must be isolated from any other websites or applications not related to the website (for example, hosting can be realized on virtual private server or containerized via a third-party hosting provider such as AWS, Google, or Microsoft Azure).

- Eurasia Foundation should be allowed to choose the geographical location of the datacenter.
- Designated Eurasia Foundation staff should have full access permissions to the hosting environment.
- The hosting environment must have monitoring and threat protection systems in place to monitor for unusual activity and activity patterns and prevent unauthorized access attempts.

- The hosting environment must allow installation of Eurasia Foundation's intrusion detection system (IDS), Alert Logic.
- The website should only be accessible through HTTPS connection using an auto-renewing SSL (TLS) certificate. The certificate must be maintained by the Vendor.
- The website must work through Eurasia Foundation's Content Distribution Network and web application security service, Cloudflare.

Part II: Website Maintenance

Provide ongoing website maintenance, including:

- Regular updates of the server and the website software as verified updates and security patches become available.
  - Upgrades must be deployed to Vendor's test servers and tested prior to production release.
- Ongoing performance and security monitoring.
  - Upon discovery of any performance and/or security issue, notifications must be sent to Client. Performance and security issues are treated as high priority/urgent, and Client is immediately notified by email and/or phone.
- Routine maintenance of the server and application software, licensing, including third-party integrations such as Single Sign-On, ADP, Cloudflare, Google Tag Manager and Analytics, and other third-party systems as applicable to ensure website's optimal and secure performance.
- Maintenance of WCAG 2.2 AA web accessibility scores in the 90+/100 range across the site. As WCAG standards are updated, our website must also update to maintain 90+/100 scores at the AA level.

Tasks related to website hosting and system administration and maintenance will not require the use of support hours, delineated below.

Part III: User Support

Provide ongoing website user support, including but not limited to:

- Requests to modify or update content, imagery, and templates.
- Password reset assistance.

Up to 50% of remaining user support hours at the end of the month should roll over to the next month.

General Requirements:

Vendor should specify regular support hours Monday to Friday, 9am to 5pm Eastern Time, excluding holidays. User support requests of a non-emergency nature can be submitted 24/7. During weekdays, Vendor will respond within 24 hours of receiving a service request, with an estimate of when the request can be completed. Vendor and Client will use a designated support management platform to submit, respond, and track Client's site issues.

Vendor will monitor and respond to emergency issues with Client website 24/7, Monday to Friday, and all-day Saturday, Sunday, and holidays. Vendor will provide Client with an emergency email address and phone number that will alert the support team when such an issue is submitted. During emergency support hours, Vendor will respond within 2 hours of receiving a request, with an estimate of when the ticket can be completed.

Vendor should provide a Service Level Agreement that specifies quality of service, availability of the website, and responsibilities.

Website hosting, maintenance and support should be performed according to a Eurasia Foundation-approved plan developed by the Vendor. The plan should include information about the support team, maintenance, and security procedures (for example: backup schedule and retention, update schedule, security services information, references to incident response and recovery protocols), security measures, response and issue resolution time, scheduled reviews of website access permissions, and other logs with the responsible Eurasia Foundation staff.

Vendor should have incident response protocol and other information security policies and procedures in place and should be willing to adjust its practices according to Eurasia Foundation's requirements if needed.

Security incident disclosure: Vendor will notify Client with undue delay after becoming aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Client data (a "security incident"). Vendor will make reasonable efforts to identify and remediate the cause of such breach, including steps to mitigate the effects and to minimize any damage resulting from the security incident.

Vendor will be required to participate in Client's disaster recovery and business continuity planning efforts, and exercises related to Client's website (www.eurasia.org) as well as annual Payment Card Industry assessments. This includes filling out annual disaster recovery and business continuity preparedness checklists, providing information to ensure resource continuity, and participating in annual tabletop recovery exercises.

Vendor must submit a monthly report outlining activities performed and metrics around, for example, unexpected behavior, security issues, and application downtime.

APPLY

Proposals must include the following:

- Written proposal (maximum six pages) that includes:
  - Detailed hosting, maintenance, and support plan.
  - An applicant's information, configuration, and cybersecurity management statement that describes how all aspects of the applicant's internal security

systems are organized to ensure integrity and security of Eurasia Foundation information assets and systems. Applicants should note relevant certifications they hold (e.g., ISO 27001, ISO 27701, SOC2, PCI DSS) as well as information on data breaches within the past 3 years, and adherence to security standards, information security policy, or recent third-party cybersecurity attestation.

- Client references (no page limit).
- Detailed budget, including one-time and monthly budget (if applicable) for providing services (no page limit).

The selection process is open and competitive, and participants will be selected based on the criteria outlined below.

- Technical solution: clarity and suitability of the applicant's approach.
- Past performance: relevance of the applicant's technical expertise and successful track record of projects delivered on time and on budget.
- Cost.

If additional information or clarification on submitted proposals is needed, the applicant(s) will be notified in writing and will be asked to submit additional information and/or documentation.

Finalists may be invited to give a presentation of their proposal and clarify technical questions prior to the announcement of the winning proposal.

Interested parties are invited to submit proposals no later than 11:59PM ET May 6, 2024.