BRAND USA

Brand USA

REQUEST FOR PROPOSAL

Project Name: Model Context Protocol (MCP) Server Setup
and Administration

Date: December 15, 2025

INTRODUCTION

As the destination marketing organization for the United States, Brand USA's mission is to increase incremental international visitation, spend, and market share to fuel the nation's economy and enhance the image of the USA worldwide.

Established by the Travel Promotion Act of 2009 as the nation's first public-private partnership to spearhead a globally coordinated marketing effort to promote the United States as a premier travel destination and communicate U.S. visa and entry policies, Brand USA began operations in May 2011.

As one of the best levers for driving economic growth, international travel to the United States currently supports 1.2 million American jobs* and benefits virtually every sector of the U.S. economy. Since its founding, Brand USA has worked with more than 900 contributing organizations to invite the world to explore the exceptional, diverse, and virtually limitless travel experiences and destinations available in the United States of America.

According to studies by Oxford Economics, over the past seven years Brand USA's marketing initiatives have helped welcome 7.5 million incremental visitors to the USA, benefiting the U.S. economy with nearly $55 billion in total economic impact, and supporting more than 50,000 incremental jobs each year.

Brand USA's operations are supported by a combination of nonfederal contributions from destinations, travel brands, and private-sector organizations plus matching funds collected by the U.S. government from international visitors who visit the United States under the Visa Waiver Program.

For industry and partner information about Brand USA, please visit TheBrandUSA.com.

For information about exceptional and unexpected travel experiences in the United States, please visit Brand USA's consumer website at VisitTheUSA.com.

PURPOSE

Brand USA seeks a secure, standardized MCP layer in GCP that (i) abstracts access to common enterprise systems (e.g., CMS, DAM, CRM, data warehouse, project/work management, file storage, event management, cloud productivity suites) via auditable tools; (ii) supports multiple top-tier model providers through a single policy-enforced gateway; and (iii) aligns with our existing security, privacy, and data governance practices. Responses should emphasize risk management, auditability, and long-term operability over experimental features.

This Request for Information (RFI) is issued solely for information and planning purposes - it does not constitute a Request for Proposal (RFP), Request for Quote (RFQ), Solicitation, or a promise to issue an RFP, RFQ, or Solicitation in the future. This RFI does not commit Brand USA to contract for any supply or service whatsoever. Further, Brand USA is not seeking proposals at this time and will not accept unsolicited proposals. Responders are advised that Brand USA will not pay for any information or administrative costs incurred in response to this RFI; all costs associated with responding to this RFI will be solely at the interested party's expense. The information provided in this RFI is subject to change and is not binding. This RFI does not restrict Brand USA's acquisition approach including but not limited to not issuing an RFP if that is deemed in the best interest of Brand USA. Responses to this RFI will not be returned and respondents will not be notified of the result of the review. In the event an RFP is issued, it will be announced on the Brand USA website at a later date, and all interested parties must respond to that RFP announcement separately from any response to this RFI.

No proprietary or confidential information should be included in your response. Participation in this RFI doesn't commit Brand USA to any future procurement activity.

BACKGROUND

Brand USA is the nation's destination marketing organization, focused on driving international visitation, increasing visitor spend, and strengthening the United States' global brand. As our digital and data programs evolve, Brand USA is exploring the integration of secure AI infrastructure to support marketing automation, analytics, and partner engagement. We are gathering information from qualified vendors to inform the next phase of our AI integration strategy, beginning with the deployment of a Model Context Protocol (MCP) Server in our Google Cloud Platform (GCP).

Brand USA's technology environment spans multiple systems, including CMS, DAM, CRM, analytics platforms, user identity systems, data warehouses, partner APIs, and a broad set of operational tools. To responsibly leverage generative AI tools, we require a secure, standardized layer that allows controlled model access to internal data.

The MCP Server will serve as that bridge---enabling trusted AI tools (e.g., OpenAI, Anthropic, or internal LLMs) to query Brand USA's data and services through structured, auditable APIs. The environment must adhere to Brand USA's security, privacy, and governance standards while remaining flexible for future AI applications.

Target Systems for Phase 1

The initial MCP implementation will connect to the following Brand USA systems:

- CMS: WordPress
- DAM: MediaValet
- CRM: Salesforce
- Data Hub
- Research Hub / PSP: [To be specified for potential partner reporting access]

User Scenarios and Access Patterns

The MCP server must support two distinct user populations with different access requirements:

Scenario A: Internal Staff (Full Context Access)

-Users: Brand USA Employees
- Interface Options:
  - Claude Desktop (primary)
  - Local IDEs for developers
  - Proprietary Chat Interface (potential)
- Access Requirements: Full querying capabilities including Data Hub analysis, CRM reporting with both read and write permissions (e.g., updating CRM records), and deep analytical access
- Security Model: Role-based access control aligned with internal permissions

Scenario B: Third-Party Partners (Restricted Context Access)

- Users External agencies, partners, B2B travel planners (business and leisure sectors)
- Interface Options:
  - Partner's own AI tools (e.g., agency using their ChatGPT Team account to query Brand USA's DAM)
  - Restricted gateway/web chat interface provided by Brand USA
  - Research Hub / PSP for approved reporting access (potential)
- Access Requirements: Read-only access to CMS and DAM content, retrieval of approved assets and public-facing content only
- Security Model: Rigid row-level security with strict data isolation to prevent access to internal-only data

Objective

(1) gather insights from vendors that can provide secure AI middleware and protocol-based integrations supporting both "bring your own client" and hosted interface models

(2) understand cloud-native approaches for deploying and operating MCP in GCP with strong guardrails (identity, network, secrets, audit) that can enforce different permission models for internal vs. external users

(3) assess Brand USA's strategy for implementation across multiple user populations and access patterns

SUBMISSION REQUIREMENTS

Please follow the outline below. At this time, Brand USA is not offering any Q&A. Vendors are encouraged to respond to this RFI based on information provided in this document.

Executive Summary (≤1 page) including risks and mitigations

Answers to RFI Questions (≤15 pages)

Optional Diagrams (≤2) showing identity, network, audit, and observability flows

Responses are due via email to **RFPAdmin@thebrandusa.com** no later than **February 02, 2026**. Respondents are reminded that this is an RFI and **IS NOT A RFP**. Responses to this notice shall not constitute responses to solicitation, which is not currently available. Brand USA will not provide Q&A, and responses will not be returned.

RFI Questions:

Company Profile

1. Provide a brief company overview, including years in business, areas of specialization, and relevant certifications (e.g., SOC 2, ISO 27001).

2. Describe your familiarity with Brand USA's existing digital ecosystem, specifically including experience with WordPress (CMS), MediaValet (DAM), Salesforce (CRM), and analytics platforms.

3. Describe what your recommended approach would be for:
   - AI middleware or protocol-driven integrations (JSON-RPC, gRPC, MCP)
   - GCP-native deployment (Cloud Run, VPC, IAP, Secret Manager, Cloud Armor)
   - Data security, privacy, and compliance frameworks
   - Supporting both "bring your own client" (e.g., Claude Desktop) and hosted interface models

4. Share relevant past work: AI infrastructure, secure API orchestration, cloud middleware, or MCP-like frameworks, particularly involving multi-tenant or partner access scenarios.

Technical Capabilities

Architecture & Deployment in GCP

- Outline the recommended MCP server architecture in GCP (e.g., Cloud Run or equivalent) including VPC design, ingress/egress controls, and isolation for tools/connectors.

- Describe your recommended identity approach for users, services, and tools (e.g., OAuth2/OIDC, workload identity, short-lived credentials), and how least-privilege will be enforced per tool for Brand USA.

- Explain how your architecture will support both internal staff using MCP-compatible clients (Claude Desktop, IDEs) and external partners using either their own AI tools or a hosted gateway.

- Describe how your solution would integrate with WordPress, MediaValet, Salesforce, and Brand USA's data/analytics systems, with minimal disruption.

Authorization & Policy

- Describe how tool access will be governed (role-/attribute-based) and how requests are evaluated before execution.

- Explain your approach to implementing differentiated permission models:
  - Internal staff: Full read/write access to appropriate systems
  - External partners: Read-only access with row-level security enforcement

- Detail how row-level security will be enforced to ensure external partners never access internal-only data, even when querying shared systems like the CMS or DAM.

Auditability & Observability

- Provide your audit/logging design (who/what/when/why), correlation IDs, and retention strategy. Include OpenTelemetry-style tracing for tool calls and model interactions, and dashboards/alerts for drift, latency, and error budgets.

- Explain how audit trails will capture the distinction between internal staff actions and external partner queries.

Data Governance Controls

- Describe how you will apply data classification and masking/redaction to PII prior to model exposure; row/column-level filtering, and lineage capture for tool outputs and prompts.

- Explain your approach to ensuring that external partners accessing the MCP server can only retrieve approved, public-facing content from the CMS and DAM.

Safety & Abuse Resistance

- Describe protections against prompt injection, data exfiltration via tools, and jailbreaks; include request validation, allow/deny lists, and output filters for sensitive data.

- Address specific risks associated with external partners using their own AI tools to query Brand USA systems.

Multi-Model Neutrality

- Explain how your approach abstracts multiple leading model providers behind a stable interface, including capability negotiation, model routing/fallback, and provider-specific tokenization/limits handling---without locking us to a single provider.

- Describe how your solution will work with partners who may use different AI providers (e.g., OpenAI, Anthropic) to access Brand USA's MCP server.

Administration & Support

1. Describe your operating model (managed, hybrid, handoff) and what remains Brand USA's responsibility.

2. What is your recommended SLA/SLO (uptime/latency)?

3. Detail patching/vulnerability management cadence, dependency tracking, and secrets rotation policy.

4. Brand USA values continuity of institutional knowledge and the ability to move quickly from discovery to implementation. Please describe how your team will ensure a short runway to value, minimizing time spent on basic discovery and orientation.

5. What administrative and maintenance models do you offer (managed service, hybrid, or handoff)?

Future Readiness

1. How would your architecture scale as Brand USA expands AI capabilities and the number of external partners accessing the system?

2. What integrations (CRM, CMS, analytics) or extensions would you prioritize for future phases beyond the Phase 1 systems (WordPress, MediaValet, Salesforce)?

3. Explain your approach to adding new tools/connectors using a repeatable template (schema, auth, policy, tests), and how API/tool versioning is handled to avoid breaking changes.

4. Describe migration strategies for model/provider changes (capability parity, fallback) with minimal downtime.

5. Describe how your solution could support multiple environments (dev/test/prod) and potentially multiple Brand USA properties or regional variants, with strong configuration and tenant isolation for both internal and external user populations.

BUDGET

Implementation services. We understand that pricing is dependent on more information. An implementation price range will be acceptable. Unreasonably wide ranges will not be considered. Brand USA is looking for realistic pricing information for budgeting purposes. State any assumptions.

  - Run/operate (include any cost drivers and unit assumptions)
  - Optional enhancements

SCHEDULE

This tentative schedule may be altered at any time at the discretion of Brand USA.

A. Proposal Released   December 15, 2025

B. Proposal Due (due by 5:00 PM EDT).   February 2, 2026

DELIVERY OF PROPOSAL

Proposals should be e-mailed to RFPadmin@TheBrandUSA.com. We will acknowledge receipt, so if you do not receive a receipt notification within two business days, please contact us.   If the file size of your proposal is too large to email, or send via a FTP service, contact us and we will make arrangements.