Request for Information (RFI)

Online Presence Vetting (OPV) Solution

U.S. Department of State

Bureau of Diplomatic Technology

IMPORTANT NOTICES

THIS IS A REQUEST FOR INFORMATION (RFI) ONLY. This RFI is issued solely for market research and information planning purposes and does not constitute a solicitation for proposals or a commitment by the Government to issue a solicitation. The Government will not pay for any information or administrative costs incurred in response to this RFI. All costs associated with responding to this RFI are solely at the responding party's expense. Responses to this RFI will not be returned. Not responding to this RFI does not preclude participation in any future solicitation. The Government reserves the right to cancel this RFI at any time without obligation to respondents.

Proprietary information submitted in response to this RFI will be safeguarded and handled in accordance with applicable Government regulations. Respondents should clearly mark any proprietary or sensitive information contained in their responses.

Section 1: General Information

1.1 Issuing Office

U.S. Department of State Bureau of Diplomatic Technology Office of Consular Systems and Technology Washington, D.C. 20520

1.2 RFI Point of Contact

All questions and responses shall be submitted electronically through email. All communications regarding this RFI must go through the Contracting Officer.

1.3 Response Submission Instructions

- All responses must be submitted electronically via email to KayaniBA@state.gov no later than 11:00 AM EST on July 10, 2026.
- Responses shall be submitted in PDF format
- Maximum response length: 40 pages excluding cover page, table of contents, and company information section
- Font: Times New Roman, minimum 12 point
- Margins: 1 inch on all sides
- File size shall not exceed 25 MB
- Responses received after the due date and time will not be reviewed

1.4 Classification and Handling

This RFI is designated Sensitive But Unclassified (SBU). Respondents shall not include classified information in their responses. If a respondent believes classified information is necessary to fully respond, they should contact the Contracting Officer for guidance.

Section 2: Background and Program Overview

2.1 Agency Mission

The U.S. Department of State's mission is to protect and promote U.S. security, prosperity, and democratic values and shape an international environment in which all Americans can thrive. The Bureau of Consular Affairs (CA) is charged with protecting and assisting U.S. citizens abroad, issuing passports to U.S. citizens, and screening foreign nationals applying for immigrant and nonimmigrant visas according to U.S. law.

2.2 Program Context

The Office of Consular Systems and Technology (CST), within the Bureau of Diplomatic Technology (DT), provides mission critical information technology resources to support more than 300 consular locations including approximately 230 overseas posts located in foreign countries, 29 domestic passport agencies, 2

domestic visa processing centers, and Washington, DC headquarters, and an array of information, book and card print, passport centers, Department of State annexes, and contractor sites. CST supports approximately 10,000 worldwide clients in over 300 locations.

2.3 Regulatory Driver

Executive Order 14161, Protecting the United States from Foreign Terrorists and Other National Security and Public Safety Threats, directs federal agencies to conduct comprehensive vetting and screening of all visa applicants to the maximum degree possible to ensure the safety of American citizens. Executive Order 14188, Additional Measures to Combat Anti-Semitism, further directs scrutiny of foreign student and exchange visitor activities. In response to these directives, the Department has issued guidance requiring comprehensive online presence vetting for visa applicants across multiple nonimmigrant visa classifications.

2.4 Program Objective

CST seeks to acquire a comprehensive Online Presence Vetting (OPV) solution to support the consular visa adjudication process and other consular work as needed. The solution must provide automated open source intelligence data collection, entity resolution, and analytical insights to enable consular officers to conduct thorough and effective online presence screening of visa applicants at a scale of up to 18 million applicants annually across more than 300 consular locations worldwide.

2.5 Operational Environment

The OPV solution will operate within the Department of State's information technology environment and must integrate with existing consular systems. The solution will be used by consular officers at posts worldwide operating across multiple time zones. The solution will require a Department of State-issued Authority to Operate.

Section 3: Requirement Overview

3.1 Core Service Areas

The Government is seeking a solution that provides three core service areas. Respondents should address their capabilities in each area.

Core Service Area 1: Data Collection Service

The solution must provide comprehensive data collection capability that aggregates open source and publicly available information about individual visa applicants from across the internet. Key requirements include:

- Comprehensive online presence coverage extending beyond listed platforms to include regional and country-specific social networks, online forums and message boards, gaming platforms, dating applications, e-commerce seller profiles, dark web-adjacent platforms, and any other publicly accessible digital surface where applicant activity may be present including but not limited to Facebook, Instagram, X (Twitter), LinkedIn, Reddit, TikTok, YouTube, Telegram, VK, Weibo, and Gab
- Extended online presence coverage beyond traditional social media including professional platforms, forums, and other online services such as academic and professional publication databases including Google Scholar, ResearchGate, PubMed, patent databases (USPTO, WIPO), and news/media archives for authored content
- Anonymous collection that does not reveal to the applicant or the platform that screening is being conducted
- Seed parameter-based searching using first name, last name, date of birth, address, email addresses, phone numbers, and social media usernames
- Historical data retrieval with a minimum five-year lookback period
- Multilingual collection and content analysis across as many world languages as possible. Detection of online presence curation or account scrubbing activity
- Ability to add coverage for new platforms within approximately 90 days of request
- Live and real-time data collection rather than reliance on cached or historical databases

- Checks against public criminal records including court dockets, arrest records, conviction databases, sex offender registries, international sanctions lists, etc
- Licensed commercial financial data aggregator integration (e.g., LexisNexis, Dun & Bradstreet, or equivalent) providing access to financial records, bankruptcy filings, liens, judgments, business ownership records, and property records
- Vital records coverage including publicly available and commercially licensed marriage, divorce, birth, and death records across domestic and international jurisdictions to support identity verification and fraud detection

Core Service Area 2: Data Entity Resolution Service

The solution must enable identities to be resolved, linked, and deconflicted across multiple platforms and data sources. Key requirements include:

- Link analysis and account discovery using seed parameters to identify undisclosed accounts
- Confidence scoring that clearly distinguishes between high confidence and low confidence matches
- Reverse image search capability using the applicant's visa photo as a query input across open web sources, image hosting platforms, news archives, and social media to identify undisclosed identities, aliases, or associations. Cross-platform identity linking using shared identifiers such as phone numbers, email addresses, usernames, and behavioral patterns
- False positive management including mechanisms for handling recycled phone numbers, common names, and shared email addresses
- Cross-referencing of applicant-provided biographical data against vital records to identify inconsistencies indicative of identity fraud, document fraud, or fraudulent family relationship claims

Core Service Area 3: Analytical Platform with Insights

The solution must provide a web-based analytical platform and API that presents collected and resolved data in a unified interface for consular officer review. Key requirements include:

- Unified dashboard aggregating all collected online presence information for each applicant
- Configurable risk indicators and filtering based on vetting criteria defined by the Department
- Content analysis across languages identifying relevant themes, sentiment, and potential indicators of inadmissibility
- Live querying capability via user interface and API
- Comprehensive audit logging of all user actions, searches, and data access
- Configurable data retention policies and automated purging capabilities
- Standardized reporting for each applicant that can be retained as part of the adjudication record

3.2 Critical Technical Requirements

The following represent mandatory capabilities that any solution must satisfy:

- API availability supporting secure automated data exchange with consular systems
- Fully automated end-to-end analysis without requiring human intervention from seed parameter ingestion through results delivery
- Demonstrated scalability to process high-volume queries at global scale supporting all consular posts worldwide
- Specialization in individual-level open source data collection and analysis
- Live record search collecting data from social media platforms in real time
- Processing time: results available within 30 minutes of seed parameter submission
- Availability: 99.9% uptime during business hours across all consular post and facility time zones (effectively 24/7)

- API acknowledgement within 5 seconds of submission
- Dedicated, isolated server infrastructure with no commingling of applicant data with other customers

3.3 Security Requirements

- Contractor personnel must possess a minimum approved Department of State Moderate Risk Public Trust for specific positions
- All data encrypted at rest and in transit using industry standard or greater encryption
- Compliance with FISMA, NIST SP 800-53, and all applicable Department of State security requirements
- Ability to achieve a Department of State-issued Authority to Operate within 6 months of contract award

Section 4: RFI Response Requirements

Respondents shall organize their responses using the section structure provided below. Each section should be clearly labeled. Responses that do not follow this structure may not be fully considered in the Government's market research analysis.

Section A: Company Information

Respondents shall provide the following information:

A1. Company Legal Name A2. Company Address A3. CAGE Code A4. Unique Entity Identifier (UEI) A5. Business Size (large business, small business, or other) A6. Applicable Socioeconomic Categories (check all that apply)

- Small Business
- Small Disadvantaged Business
- 8(a) Certified

- Woman-Owned Small Business (WOSB)
- Economically Disadvantaged Woman-Owned Small Business (EDWOSB)
- Service-Disabled Veteran-Owned Small Business (SDVOSB)
- HUBZone Small Business
- None of the above

A7. Number of Employees (total company) A8. Approximate Annual Revenue A9. Current Facility Clearance Level (if applicable) A10. Primary Point of Contact

- Name
- Title
- Phone Number
- Email Address

A11. Secondary Point of Contact

- Name
- Title
- Phone Number
- Email Address

A12. Company Website

Section B: Capability Statement

Respondents shall provide a capability statement describing their organization's ability to meet the OPV requirements. The capability statement shall address each of the three core service areas separately.

B1. Data Collection Service Capability

B1.1 Social Media Platform Coverage Provide a complete list of all social media and online platforms currently supported by your solution. For each platform, indicate the platform name, type of content collected, depth of collection and any

known limitations on collection. Additionally, identify any platforms relevant to visa applicant vetting that your solutions do not currently cover, and the reason. Provide platforms on your near-term roadmap for new or restored coverage, including expected availability dates.

B1.2 Criminal Records Coverage Identify all criminal record databases, court record systems, sanctions lists, and law enforcement-adjacent open sources currently covered by your solution. Describe the jurisdictional coverage (federal, state/local, international) and any known gaps.

B1.3 Commercial Financial Data Aggregator Integration Identify any licensed commercial data providers integrated into your solution (e.g., LexisNexis, Dun & Bradstreet, Equifax). Describe the data types available, jurisdictional coverage, refresh frequency, and any licensing or access restrictions that may affect Government use.

B1.4 Publications Coverage Describe your capability to collect and analyze academic, professional, and media publications authored by or referencing the applicant. What databases and archives are covered? How does your solution identify co-authors, institutional affiliations, and funding sources disclosed in publications?

B1.5 Comprehensive Online Presence Coverage Beyond the platforms explicitly listed, describe your solution's capability to identify and collect data from the full spectrum of an applicant's online presence, including regional platforms, niche forums, gaming networks, and other non-traditional digital surfaces. How does your solution discover platforms not initially seeded by the Government?

B1.6 Vital Records Coverage Describe your solution's access to marriage, divorce, birth, and death records. What jurisdictions are covered domestically and internationally? What commercial data providers supply this data? How does your solution flag discrepancies between applicant-provided information and vital records findings?

B1.7 Real-Time Collection Describe your approach to live, real-time data collection. Explain how your solution collects data directly from platforms rather than relying on cached databases or third-party data sources. Describe the currency of data returned and any factors that affect data freshness.

B1.8 Anonymous Collection Describe your approach to anonymous data collection. Explain how your solution prevents platforms from identifying that screening is being conducted. Describe the infrastructure you maintain to ensure continuous, uninterrupted access to target platforms. Address how you handle platform bans, rate limiting, and access restrictions.

B1.9 Seed Parameter Processing Describe how your solution processes seed parameters to identify and collect relevant online presence data. Address how your solution handles partial information, common names, and ambiguous identifiers.

B1.10 Historical Data Retrieval Describe your historical data retrieval capabilities. What is the maximum lookback period your solution supports? How is historical data stored and retrieved? What are the limitations of historical data retrieval for each major platform?

B1.11 Multilingual Capabilities List all languages currently supported by your solution for both data collection and content analysis. Describe your approach to languages using non-Latin scripts including Arabic, Chinese (Simplified and Traditional), Cyrillic (various languages), Korean, Japanese, Farsi, Urdu, and others. Describe how your solution handles translation and whether translation services are integrated or require a separate vendor.

B1.12 Account Scrubbing Detection Describe your capability to detect evidence of online presence curation or account scrubbing. What indicators does your solution use to identify this activity? How are these findings presented to the reviewer?

B1.13 New Platform Integration Describe your process for adding coverage for new platforms. What is your current average timeline for integrating a new platform? What factors affect this timeline? Can you commit to adding new platforms within 90 days of request?

B1.14 Throughput and Capacity Provide documented evidence of your solution's current data collection capacity including:

- Maximum number of applicants processed per day
- Maximum number of concurrent queries
- API rate limits

- Processing time from seed parameter submission to results delivery
- Any factors that affect processing speed or capacity

B2. Entity Resolution Service Capability

B2.1 Link Analysis and Account Discovery Describe your link analysis methodology for discovering undisclosed accounts and online activity. How does your solution identify connections between seed parameters and both disclosed and undisclosed online accounts? Provide examples of the types of connections your solution can identify.

B2.2 Confidence Scoring Describe your confidence scoring methodology. How does your solution assign confidence scores to entity matches? What thresholds distinguish high confidence matches from low confidence matches? How are confidence scores presented to the reviewer? Can confidence thresholds be adjusted by the customer?

B2.3 Facial Recognition and Image Matching Describe your facial recognition and image matching capabilities including:

- Technology and algorithm used
- Current accuracy rate for standard quality images
- Performance with low quality images such as visa photos
- False positive rate for facial recognition matches
- Platforms and image sources currently searched
- Compliance with applicable facial recognition regulations and guidelines

B2.4 Cross-Platform Identity Linking Describe how your solution links accounts belonging to the same individual across different platforms. What shared identifiers does your solution use? How does your solution handle cases where shared identifiers are absent? Describe your behavioral pattern analysis capabilities.

B2.5 False Positive Management Describe your approach to managing and reducing false positives. How does your solution handle common names, recycled phone numbers, and shared email addresses? What mechanisms exist for reviewers to flag and correct false positive matches? How quickly can match thresholds be

adjusted? Describe how your solution handles common name collisions in vital records searches and how it distinguishes between records belonging to the applicant versus unrelated individuals with similar biographical data.

B3. Analytical Platform Capability

B3.1 User Interface and Dashboard Describe your web-based analytical platform and unified dashboard. How is information organized and presented for consular officer review? Provide screenshots or mockups if available and not proprietary.

B3.2 Risk Indicators and Filtering Describe your risk indicator and filtering capabilities. How are risk indicators defined and configured? Can risk filters be customized by the customer? How are risk flags presented to the reviewer?

B3.3 Content Analysis Describe your content analysis capabilities including:

- Sentiment analysis methodology
- Theme identification and categorization
- Language support for content analysis
- Identification of potential indicators of inadmissibility
- How content analysis findings are presented to the reviewer
- Identification of references to criminal activity, legal proceedings, or law enforcement encounters within collected content
- Analysis of publication content for indicators of concern including affiliations with sanctioned institutions, foreign government or military funding, and technology areas subject to export controls

B3.4 API Capabilities and Integration Experience

Describe your API capabilities in detail including:

- Available endpoints and their functions
- Authentication methods supported
- Batch upload capabilities and formats
- Results retrieval mechanisms (push via webhook and pull via polling)

- API rate limits and throughput
- API response time benchmarks
- API documentation availability
- Sandbox or test environment availability

Additionally, describe your proven experience integrating your API with external client systems, including:

- Number of successful API integrations completed with government or commercial customers
- Types of client systems integrated with (case management, identity management, workflow/adjudication systems, data warehouses, etc.)
- Typical integration timeline from kickoff to production cutover
- Integration support model (dedicated integration engineers, professional services, customer self-service, etc.)
- Common integration challenges encountered and how they were resolved
- Customer references that can speak to the integration experience

B3.5 Audit Logging and Compliance Describe your audit logging capabilities. What user actions, searches, and data access events are logged? How long are audit logs retained? How can audit logs be accessed and exported?

B3.6 Data Retention and Purging Describe your data retention and purging capabilities. Can retention periods be configured by the customer? How is automated purging implemented? How is data destruction certified?

B3.7 Reporting Describe the standardized reports your solution generates for each applicant. What information is included in the report? In what formats can reports be exported? Can report templates be customized?

Section C: Technical Approach Questions

Respondents shall provide specific answers to the following technical questions.

C1. Scalability The Government requires a solution capable of processing up to 18 million applicants annually across more than 300 consular locations worldwide. Describe how your solution scales to meet this requirement. Provide documented evidence of the largest scale at which your solution has been deployed. What infrastructure investments would be required to support this volume? What is your current maximum demonstrated throughput?

C2. Processing Time The Government requires results to be available within 30 minutes of seed parameter submission for standard batch processing. Describe your current average processing times. What factors affect processing speed? Under what circumstances might processing exceed 30 minutes? How does your solution handle processing time SLA violations?

C3. Dedicated Infrastructure The Government requires dedicated, isolated server infrastructure with no commingling of applicant data with other customers. Describe your ability to provide dedicated infrastructure for a single government customer. Where would this infrastructure be physically located? Is all infrastructure located on U.S. soil? Describe your experience providing dedicated infrastructure to government customers.

C4. Authority to Operate Describe your experience obtaining Authority to Operate from federal agencies. Have you previously obtained an ATO from the Department of State or other federal agencies? Do you currently operate in a FedRAMP authorized environment? What is your estimated timeline to achieve a Department of State-issued ATO? What challenges do you anticipate in the ATO process for this requirement?

C5. Security Clearances Does your organization currently hold a facility clearance? If so, at what level? What percentage of your workforce holds active personnel security clearances at the SECRET level or above? Describe your experience working on classified government programs. What is your current capacity to onboard cleared personnel for a new program?

C6. Integration with Government Systems Describe your experience integrating with government consular or immigration systems. What integration challenges do you anticipate for this requirement? What information would you need from the

Government to plan and execute integration? What is your estimated timeline for completing integration with existing consular systems?

C7. Platform Terms of Service Compliance Many social media platforms prohibit automated data collection in their Terms of Service. Describe how your solution addresses Terms of Service compliance. What legal authorities or agreements does your organization have with social media platforms? How do you manage the legal risk associated with automated data collection? Have you ever faced legal action from a platform related to data collection activities?

C8. Multilingual Content Analysis Describe your multilingual content analysis capabilities in detail. How does your solution identify and analyze content in languages other than English? What is the accuracy of your content analysis across different languages? How does your solution handle code-switching, slang, and culturally specific references?

C9. Artificial Intelligence and Algorithm Transparency Describe the artificial intelligence and machine learning components of your solution. How does your solution explain risk scores and content analysis findings to reviewers? What steps do you take to identify and mitigate bias in your algorithms? How are your models validated and updated? What human review mechanisms exist for AI-generated findings?

C10. Data Governance and Privacy Describe your data governance framework. How do you ensure applicant data is used only for the purposes specified in the contract? What restrictions exist on your use of government data for AI model training or other purposes? How do you handle data collected on U.S. persons inadvertently captured during applicant screening? Describe your data destruction and certification processes.

C11. Describe any data rights, intellectual property, or proprietary restrictions that may apply to your proposed solution or approach. Identify any commercial items, technical data, or computer software that would be subject to restricted rights, and explain how these restrictions might impact the Government's ability to use, modify, or maintain the solution.

C12. How does your solution manage data obtained through commercial licensing agreements (e.g., LexisNexis)? Are there contractual restrictions on Government use of this data? How are licensing costs passed through to the Government?

Section D: Past Performance

Respondents shall provide information on up to five relevant past or current contracts. For each contract, provide the following information:

D1. Contract Information

- Contract Name
- Contract Number
- Contracting Agency
- Period of Performance (start and end dates)
- Contract Value (total)
- Contract Type (FFP, T&M, IDIQ, other)
- Current Status (active or completed)

D2. Work Description Provide a brief description of the work performed and its relevance to the OPV requirement. Address the following:

- Type of data collected and analyzed
- Number of individuals screened or processed
- Platforms and data sources covered
- Scale of operations (queries per day, applicants per year)
- Security clearance requirements
- ATO or equivalent authorization obtained

D3. Government Point of Contact

- Name

- Title
- Agency
- Phone Number
- Email Address
- Relationship to Contract (COR, CO, Program Manager, other)

D4. Relevance Assessment Rate the relevance of this contract to the OPV requirement and explain your rating:

- Highly Relevant: Work is essentially the same as the OPV requirement
- Relevant: Work is similar in nature, scope, or complexity to the OPV requirement
- Somewhat Relevant: Work has some similarities to the OPV requirement

Respondents are specifically encouraged to identify past performance in the following areas:

- Government visa or immigration vetting programs
- Law enforcement or intelligence community OSINT programs
- Large-scale individual screening programs at volumes exceeding 1 million individuals annually
- Programs requiring TOP SECRET facility clearances
- Programs requiring federal agency Authority to Operate
- Programs involving multilingual content analysis
- Programs involving facial recognition at scale

Section E: Pricing and Business Model

The Government is seeking rough order of magnitude pricing information to support development of the Independent Government Cost Estimate. Responses to

this section are not binding offers and will not be used for source selection purposes.

E1. Pricing Model Describe your preferred pricing model for this type of requirement. Address the following options and indicate which you recommend and why:

- Per query pricing
- Per applicant pricing
- Annual subscription pricing
- Tiered pricing based on volume
- Hybrid pricing model
- Other pricing model

E2. Rough Order of Magnitude Pricing Provide rough order of magnitude pricing for the following scenarios. Pricing should include all costs necessary to deliver a fully operational solution including infrastructure, software, integration, training, and support.

Scenario A: 5 million applicants per year

- Annual cost estimate:
- Cost per applicant:
- Key cost drivers:

Scenario B: 10 million applicants per year

- Annual cost estimate:
- Cost per applicant:
- Key cost drivers:

Scenario C: 18 million applicants per year

- Annual cost estimate:
- Cost per applicant:

- Key cost drivers:

E3. Infrastructure Pricing Describe the cost implications of dedicated versus shared infrastructure. What is the approximate cost premium for dedicated, isolated infrastructure? What infrastructure costs are fixed versus variable?

E4. Optional Services Pricing Provide rough order of magnitude pricing for the following optional services:

- Adding a new platform to coverage
- Surge capacity beyond baseline volume
- Additional training sessions
- Enhanced support or help desk services
- Custom report development

E5. Period of Performance Pricing The anticipated period of performance is 24 months total consisting of a 6-month base period, a 6-month option period, and a 12-month option period. Describe any pricing implications of this structure. Are there startup or implementation costs that would be incurred in the base period? How does pricing change across option periods?

E6. Cost Drivers Identify the top five cost drivers for this type of solution and describe how each affects overall pricing.

E7. Small Business Subcontracting Describe opportunities for small business participation in this requirement. What percentage of work could be subcontracted to small businesses? What types of work are most suitable for small business subcontractors?

Section F: Acquisition Strategy Feedback

The Government values industry feedback on the proposed acquisition approach. Respondents are encouraged to provide candid and specific feedback on the following topics.

F1. Period of Performance Is the proposed period of performance of 24 months total sufficient to deliver a fully operational solution supporting all consular posts worldwide? If not, what period of performance would you recommend and why?

F2. Base Period Feasibility Is the 6-month base period sufficient to achieve a Department of State Authority to Operate and deliver a minimally viable product? What are the greatest risks to meeting this timeline? What actions could the Government take to reduce these risks?

F3. Requirements Feasibility Are there any requirements that are technically infeasible or that would significantly limit competition? If so, identify the specific requirement and describe the challenge. Propose alternative approaches that would meet the Government's underlying need.

Specific to metrics, the Government is in the process of defining performance-based metrics for the Online Presence Vetting (OPV) solution, using measurable and objective standards that will form the basis of contractual Service Level Agreements (SLAs). These metrics are intended to ensure accountability, operational reliability, and mission effectiveness across all consular locations worldwide.

Are there any suggested metrics and/or acceptance criteria or acceptable quality limits the Government should consider?

F4. Requirements Clarity Are there any requirements that are unclear or that could be interpreted in multiple ways? If so, identify the specific requirement and describe the ambiguity. Propose clarifying language.

What North American Industry Classification System (NAICS) code(s) most accurately represents the work described in this requirement? Please provide a brief justification for your recommendation.

F5. Contract Vehicle What acquisition vehicle or contract type would best support this requirement? What evaluation criteria/performance incentives would best support this requirement?

Are there existing government-wide acquisition contracts (GWACs), multiple award contracts, or other contract vehicles that could be leveraged to accelerate

this acquisition? Examples include but are not limited to GSA Schedules, NASA SEWP, CIO-SP3, Alliant 2, or agency-specific vehicles.

F6. Describe your recommended phased deployment approach from contract award to full operational capability. What is the recommended phasing structure and the rationale for that structure? Provide suggested criteria for selecting initial pilot posts. Provide duration of each phase and key milestones and exist criteria to advance to the next phase.

F7. Operational Timeline What is a realistic timeline from contract award to full operational capability supporting all consular posts worldwide? What are the critical path items that most affect this timeline?

F8. Legal and Regulatory Concerns Are there any legal, regulatory, or technical concerns with the stated requirements that the Government should be aware of? This includes but is not limited to concerns related to platform Terms of Service, Computer Fraud and Abuse Act compliance, privacy regulations, or international law.

F9. Competitive Landscape In your assessment, how many vendors are capable of meeting the full scope of OPV requirements as described? Are there specific requirements that would significantly limit the number of capable vendors? What requirements, if modified, would increase competition without compromising the Government's mission needs?

F10. Small Business Considerations Can small businesses perform this requirement as a prime contractor? If not, what specific capabilities are beyond small business capacity? What set-aside or partial set-aside approaches might be appropriate for this requirement?

F11. Additional Recommendations Provide any additional recommendations, observations, or concerns regarding the OPV requirement, draft requirements, or proposed acquisition approach that were not addressed in the sections above. The Government welcomes candid feedback that will help shape a successful acquisition.

Section G: Teaming and Subcontracting

G1. Prime Contractor Intent Does your organization intend to pursue this requirement as a prime contractor, subcontractor, or both? Explain your rationale.

G2. Teaming Arrangements Are you currently in discussions with potential teaming partners for this requirement? If so, describe the general nature of the teaming arrangement without identifying specific companies. What capabilities would you seek in a teaming partner?

G3. Capability Gaps Are there any OPV requirements that your organization cannot currently meet independently? If so, identify the capability gap and describe how you would address it through teaming, subcontracting, or capability development.

G4. Subcontracting Opportunities Describe the subcontracting opportunities available within this requirement. What types of work are most suitable for subcontractors? What is your estimated subcontracting percentage?

Section 5: Terms and Conditions

5.1 No Obligation

This RFI does not obligate the Government to issue a solicitation or award a contract. The Government reserves the right to cancel this RFI at any time without obligation to respondents.

5.2 No Reimbursement

The Government will not reimburse respondents for any costs incurred in preparing or submitting responses to this RFI.

5.3 Proprietary Information

Respondents should clearly mark any proprietary or sensitive business information contained in their responses. The Government will handle marked proprietary information in accordance with applicable regulations. Respondents are advised that the Government cannot guarantee the confidentiality of information submitted in response to this RFI.

5.4 Public Disclosure

Responses to this RFI may be subject to disclosure under the Freedom of Information Act. Respondents who believe their responses contain information exempt from disclosure should clearly identify and justify any claimed exemptions.

5.5 Future Competition

Participation or non-participation in this RFI will not affect a vendor's eligibility to participate in any future solicitation related to this requirement. The Government will not use RFI responses to evaluate vendors for source selection purposes.

5.6 Government Use of Responses

Responses to this RFI will be used solely for market research purposes to inform acquisition planning. The Government may contact respondents for clarification of their responses. The Government may share anonymized or aggregated findings from RFI responses with other Government stakeholders involved in acquisition planning.

5.7 Communications

All communications regarding this RFI must be directed to the Contracting Officer. Direct contact with program office personnel is not permitted and may result in disqualification from future competition.

5.8 Conflicts of Interest

Respondents are advised that participation in market research activities including this RFI may create organizational conflicts of interest that could affect eligibility to compete for the resulting contract. Respondents with concerns about potential conflicts of interest should consult with their legal counsel.

Section 6: Attachments

Attachment A: Response Template

A Microsoft Word response template is provided to assist respondents in organizing their responses. Use of the template is encouraged but not required.