United States Department of the Interior

INTERIOR BUSINESS CENTER
Washington, DC 20240

Request for Information (RFI) / Sources Sought Notice

Artificial Intelligence (AI) Chatbot Services to Enhance Agency Recruitment Efforts
Department of the Interior, Interior Business Center (IBC)
On behalf of the Peace Corps – Office of Volunteer Recruitment and Selection (VRS)

- **RESPONSE DEADLINE: December 23, 2025, 5:00 PM Eastern Time**
- **NAICS: 54151 – Other Computer Related Services**
- **PSC: DA10 IT and Telecom - Business Application/Application Development Software as A Service**

THIS IS A SOURCES SOUGHT NOTICE. NO SOLICITATION IS AVAILABLE AT THIS TIME.

The purpose of this Sources Sought Notice is to identify potential sources capable of performing the effort described herein pursuant to FAR part 10, Market Research. This is for planning purposes only.

Any information submitted by respondents to this Source Sought Notice is voluntary. The Government does not intend to award a contract on the basis of this notice or to otherwise pay for the information solicited. Neither unsolicited proposals nor any other kinds of offers will be considered in response to this RFI. Respondents should not construe this notice as a commitment by the Government.

If the vendor believes that their response contains trade secrets or confidential commercial or financial information exempt from disclosure under the Freedom of Information Act, (5 U.S.C. 552), the cover page of their response shall be marked with the following legend: *The information specifically identified on pages ____________ of this response constitutes trade secrets or confidential commercial and financial information which the vendor believes to be exempt from disclosure under the Freedom of Information Act. The offeror requests that this information not be disclosed to the public, except as may be required by law. The vendor also requests that this information not be used in whole or part by the government for any purpose other than market research.*

1. DESCRIPTION

The Department of the Interior (DOI), Interior Business Center (IBC), on behalf of the Peace Corps Office of Volunteer Recruitment and Selection (VRS), is conducting market research to identify qualified vendors capable of providing Artificial Intelligence (AI) chatbot services to enhance recruitment, improve applicant engagement, and deliver accurate, knowledge-grounded information to prospective Peace Corps Volunteers.

2. INDUSTRY DAY ANNOUNCEMENT

The Government intends to host an Industry Day between January 7–16, 2026. A follow-on announcement will provide the confirmed date, format, agenda, and registration instructions. Interested vendors should indicate their interest in attending as part of their RFI response.

3. OBJECTIVE

The Government seeks information on vendor capabilities to provide, implement, and support a secure, accessible, knowledge-grounded AI chatbot solution that may include:

- Integration with a Wagtail/Django-based public website
- Retrieval-Augmented Generation (RAG) using Peace Corps-curated content
- Live agent escalation via CRM/ticketing tools
- Human-in-the-loop oversight and tuning
- Data protection, privacy controls, and compliance with Section 508, WCAG 2.1 AA, and FedRAMP

Responses will assist the Government in refining requirements and shaping future acquisition planning.

4. REQUESTED INFORMATION

Respondents are invited to submit:

- Company information, business size, UEI, and contract vehicles (GWAC or IDIQ) with chatbot services currently provided under the contract(s)
- Relevant AI chatbot experience
- Technical capabilities (integrations, RAG, governance, security)
- Accessibility, privacy, and compliance posture
- Implementation approach and support services
- Estimates pricing range for different options
- Interest in the planned Industry Day

5. RESPONSE INSTRUCTIONS

Submit responses in Microsoft Word format via email to:

- Michael McGuire, Contracting Officer – mike_mcguire@ibc.doi.gov
- Jacqueline Hernandez, Contract Specialist – jacqueline_hernandez@ibc.doi.gov

Subject Line: "RFI – AI Chatbot Services"
Deadline: December 23, 2025, 5:00 PM Eastern Time

Proprietary information must be clearly marked.

6. DISCLAIMER

This notice is for market research only. It does not obligate the Government to issue a solicitation or award a contract. No reimbursement will be made for any costs associated with responding.

PERFORMANCE WORK STATEMENT (PWS)

PEACE CORPS

The Office of Volunteer Recruitment and Service (VRS)

VRS AI Chatbot Services to enhance agency Recruitment Efforts

Date: November 21, 2025

Contents

2.0 GENERAL

2.1 BACKGROUND

On March 1, 1961, President John F. Kennedy established the United States Peace Corps to promote world peace and friendship. The Peace Corps' mission has three simple goals:

- Helping people of interested countries in meeting their needs for trained men and women.
- Helping promote a better understanding of Americans on the part of the people served.
- Helping promote a better understanding of other peoples on the part of Americans.

Since its founding, the Peace Corps has served in 140 developing countries, and more than 240,000 American citizens have served as Peace Corps Volunteers (PCVs).

Currently, the Peace Corps (the Agency) has over 3,200 Volunteers working with local communities in 56 host countries (Posts) in six sectors: agriculture, community economic development, education, environment, health and youth in development. Most Volunteers serve for a term of 2 years (today, this is called the PCV program). A smaller number of Volunteers serve for shorter 3 – 12-month renewable assignments and have more advanced skills (these are the Peace Corps Response (PCR) and Global Health Services Partnership (GHSP) programs). In addition, Peace Corps now offers remote volunteering opportunities through the Virtual Service Pilot (VSP) program.

The Peace Corps has approximately 2,500 employees: around 350 work in the United States, and more than 2,200 work overseas at Posts throughout the world. The Office of Volunteer Recruitment and Service (VRS) is responsible for recruiting candidates for 2-year volunteer positions, and Peace Corps Response (PCR) is responsible for the 3-12 month and virtual positions.

In the past decade, especially with the acceleration prompted by the COVID pandemic, Peace Corps staff have embraced a more virtual and mobile work environment. This shift necessitates advanced, accessible recruitment strategies to meet the evolving expectations of both staff and potential volunteers. In addition, the U.S. Office of Personnel Management (OPM) is encouraging Federal agencies to implement and incorporate leading-edge, proactive strategies and technologies.

Peace Corps has already successfully implemented an automated marketing system that lives natively in the Agency's Customer Relationship Management (CRM) system, where all current lead interactions are initiated and recorded. This system facilitates outreach through email, events, video conferences, web forms and, to a limited extent, text. Peace Corps is aiming to increase interactions with leads through more channels, specifically AI chat, meeting the next generation of Peace Corps Volunteers wherever they prefer, in a consistent voice and manner, regardless of the form of outreach. This includes, but is not limited to, highlighting opportunities to segmented audiences, reminding people of upcoming deadlines, answering commonly asked questions, appropriately directing the public to the right resource or person, and assisting potential applicants in a variety of other ways.

2.2 SCOPE

With this desire for increased outreach and flexibility, the Peace Corps is committed to improving customer service for potential applicants and stakeholders by implementing public facing, web-based AI (Artificial Intelligence) chat functionalities into its existing recruitment efforts and systems. This solicitation is for the acquisition of licenses and services to implement and integrate an AI chatbot into the www.peacecorps.gov environment. Training of the Peace Corps staff in the new system shall also be required.

2.2.1 Period of Performance

The period of performance of this task order is for one base year with two 12-month option periods for a total of three years if all optional periods are exercised. The Peace Corps will communicate the intent to exercise optional periods of performance to the Contractor in advance of the expiration of the previous period of performance.

2.3 OBJECTIVE

Through the implementation of the integrated AI chat service, the Peace Corps expects to:

- Facilitate more effective and efficient interactions between potential applicants with recruiters and the marketing team.
- Generate new leads through additional marketing channels.
- Provide smoother and more seamless interactions between the general public and relevant Peace Corps staff.
- Increase the number of leads converted into applicants through better just-in-time communications.
- Decrease the time and effort Peace Corps staff spend responding to commonly asked questions and requests for guidance from the public that can be answered through thoughtfully constructed technology.

2.4 OPTIONS

N/A

3.0 REQUIREMENTS/TASKS

3.1 TWO-WAY COMMUNICATION SERVICE SOLUTION REQUIREMENTS

3.1.1 FedRAMP Moderate Authorization

The Contractor shall provide a FedRAMP Moderate Authorization approved, commercially available, AI messaging capabilities necessary to enable two-way communication between the Peace Corps and the public. This service solution will be referred to as the “Chatbot” throughout the remainder of this performance work statement.

3.1.2 Integration with Peace Corps Website and Internal Documentation

The Chatbot shall integrate with Peace Corps website, www.peacecorps.gov, built on the Wagtail/Django Content Management Systems (CMS). To prevent hallucinations and misguidance, the Chabot's AI shall access and rely solely on source material curated by Peace Corps.

The Chatbot shall adhere to the agency's data protection protocols, ensuring that sensitive information is handled securely and in compliance with applicable regulations.

3.1.1 Continuous Learning and Optimization

The Chatbot shall include continuous learning mechanisms to improve responses over time. This includes real-time learning from user interactions, feedback loops for content updates, and regular optimization of the Chatbot's knowledge base and interaction flows to align with evolving organizational needs and priorities. The learning model should be flexible, allowing for updates based on policy changes, new user data, and advancements in AI technology.

3.1.2 User Experience

The Chatbot shall identify itself as a bot to Users, but interact and provide guidance in a voice and manner consistent with Peace Corps' values and ethos. Users shall feel a sense of continuity and personalization whether they are interacting with the Peace Corps via chatbot, the website, email, or a person.

3.1.3 Modifying and Retrieving Knowledge Dataset

The solution shall allow the Peace Corps to add, modify or edit the propriety dataset that the Chatbot uses for its knowledge base, without significant disruptions to the service. The Chatbot shall use Retrieval-Augmented Generation (RAG) techniques to ensure all responses are grounded in Peace Corps' data.

3.1.4 Natural Language Processing (NLP)

The Chatbot shall have advanced Natural Language Processing (NLP) capabilities to accurately understand, interpret, and respond to user inquiries in natural language. The solution shall handle a wide range of topics relevant to the agency's mission and user needs, ensuring efficient, engaging, and contextually appropriate user experience. All source material used by the AI shall be limited to Peace Corps' propriety dataset, to prevent hallucinations and incorrect answers.

3.1.5 Live Agent or Customer Service Transfer

The Chatbot shall ensure a seamless integration for transferring users to a live agent or customer service representative when needed. This feature must be easily accessible to users and operate without significant delays, ensuring a smooth transition from automated to human support. Additionally, the Chatbot shall contain robust queue management protocols, including real-time tracking of user positions in the queue, estimated wait times, and notifications if delays occur, and, when live support is not available, call back capabilities for the next business day. End users shall have the option to request a callback or remain in the queue. Queue management must also include mechanisms for load balancing among available agents to optimize response times and ensure efficient distribution of inquiries across the customer service team.

3.1.6 Innovation and Scalability

The Chatbot shall ensure that the communications service is scalable to accommodate for future features and capabilities. The Chatbot shall support an increasing number of users and a higher volume of interactions over time.

3.1.7 Compliance with Legal and Ethical Standards

The Chatbot shall comply with all relevant legal and ethical standards, including but not limited to the AI in Government Act, the Federal Data Strategy, and applicable privacy laws such as the California Consumer Privacy Act (CCPA). The Chatbot shall also adhere to the agency's AI governance framework, ensuring ethical use, fairness, and non-discrimination in all interactions.

3.1.8 Fair and Non-Discriminatory Operation

The Chatbot shall operate in a fair and non-discriminatory manner, and shall abide by the requirements of all applicable federal statutes, regulations and government-wide policies, such as but not limited to Title VI of the Civil Rights Act of 1964 and Obligations of Contractors and Subcontractors. The communication solution must be designed to treat all users equally, without bias or discrimination based on race, gender, age, religion, disability, sexual orientation, or any other protected characteristic. Regular audits and testing must be conducted to identify and mitigate any potential biases in the system's responses or interactions.

3.1.9 Emergency Response and User Safety

The Chatbot shall implement safety protocols to detect and respond to emergencies, such as language or behavior indicating a user is in immediate danger (e.g., self-harm). The communication solution must be capable of guiding users to appropriate resources, such as emergency services or hotlines, and must ensure that such interactions are handled with utmost sensitivity and care.

3.1.10 Human Oversight

The Chatbot shall ensure that the solution operates under appropriate human oversight, particularly in scenarios where AI responses may affect user rights or safety. The solution must incorporate checkpoints where human intervention is required, especially in situations that could have significant implications for users. All actions or responses generated by the AI that impact users must be documented and reviewed by authorized personnel to ensure adherence to agency policies and regulations.

3.1.11 Analytics and Reporting

The Chatbot shall include comprehensive analytics and reporting capabilities to track user engagement across all channels. To offer insights into user behavior and interaction patterns, enabling data-driven decisions to enhance communication strategies and messaging usage.

3.1.11.1 *Key Performance Indicators (KPI) Dashboard*

The Chatbot shall contain a live dashboard or regular reports that monitor the Key Performance Indicators (KPIs), including user satisfaction, response accuracy, and adoption rates.

3.1.11.2 *Usage Report*

The Chatbot shall contain a live dashboard or regular reports that monitor usage. If necessary, the Chatbot shall have the capability to notify designated Peace Corps staff when messaging usage has reached a certain threshold.

3.1.12 AI Risk Management

The Chatbot shall ensure that the effective management of risks associated with the use of AI technologies. This includes identifying, evaluating, and mitigating potential risks, such as unintended consequences, algorithmic biases, and ensuring compliance with federal and agency-specific AI guidelines.

3.1.13 Transparency and Accountability

The Chatbot shall maintain transparency in all AI operations, clearly informing users when they are interacting with an AI system. The Chatbot shall ensure that all AI-driven decisions and suggestions are explainable, providing users and agency personnel with understandable rationales for the outputs.

3.1.14 Data Collection, Retention, and Usage

The Chatbot shall ensure that all data collected is handled in accordance with the agency's data governance policies. Data must be stored and segmented securely, with clear protocols for temporary and long-term storage and have protections in place such as Separate Data Streams, Private Chat Windows, Data Masking Mechanisms and or Redaction Tools. The Chatbot shall adhere to Peace Corps data retention policies that dictate how long data is stored, with options for secure deletion or anonymization at the end of the retention period. User consent must be obtained for data collection by the Chatbot, and users should be informed by the Chatbot about the type of data being collected and its intended use.

3.1.15 Protected Communications Compliance

The Chatbot shall adhere to the highest standards of security and privacy, ensuring that all user communications are protected. The service shall comply with relevant federal regulations and data protection laws, safeguarding user information and maintaining the integrity of communications.

3.2 CHATBOT SOLUTION REQUIREMENTS

3.2.1 Integration with Peace Corps Website and CRM

The Chatbot shall appear to reside natively in peacecorps.gov, seamlessly available to members of the public engaging with Peace Corps content. To prevent hallucinations and misguidance, the AI shall access and rely solely on source material curated by Peace Corps.

3.2.1 Continuous Learning and Optimization

The Chatbot shall include continuous learning mechanisms to improve chatbot responses over time. This includes real-time learning from user interactions, feedback loops for content updates, and regular optimization of the Chatbot's knowledge base and interaction flows to align with evolving organizational needs and priorities. The Chatbot's learning model should be flexible, allowing for updates based on policy changes, new user data, and advancements in AI technology.

3.2.1 Data Privacy and Security

The Chatbot shall include FIPS 140-2 compliant encryption of sensitive information both in transit and at rest, secure session management, and compliance with federal and agency-specific data protection regulations. The Chatbot shall adhere to data minimization principles, retaining only the necessary data to fulfill its operational purpose, and securely deleting or anonymizing data according to retention policies.

3.3 PROJECT MANAGEMENT TASKS

3.3.1 Post- Award Kickoff Meeting

Within 10 business days of the start of performance, the Contractor will conduct a virtual post-award kickoff meeting. Specific date and time to be mutually agreed upon.

3.3.2 Quality Control Plan

The Contractor shall create a Quality Control Plan (QCP) covering all task areas and deliverables in accordance with this PWS within 15 days after the start of performance and the final QCP for acceptance within 30 days after the start of performance to the COR and the Contracting Officer. The plan shall demonstrate how the Contractor shall ensure quality performance and satisfy the requirements of the PWS.

3.3.3 Project Plan

The Contractor shall develop an initial Project Plan within 15 days after the start of performance for the implementation and operation of the proposed products, including timelines, resource requirements utilization and milestone dates. The project plan shall also allow for the Agency's change management and security review processes.

The Contractor shall maintain and update the project plan to reflect the status of the contract activities and projected milestone completion dates. Changes to the project plan shall be noted in the Status report deliverable.

3.3.4 Requirements Specification Document

The Contractor shall develop a detailed Requirements Specification Document that captures all functional and non-functional requirements for the communication services. This document must be reviewed and approved by the agency before the design phase begins. Delivery is expected within 30 days after the kickoff meeting.

3.3.5 Design and Architecture Documentation

The Contractor shall provide a Design and Architecture Document that details the technical design, system architecture, integration points, and data flows for the Chatbot. This document must be delivered within 45 days following the approval of the Requirements Specification Document. The design documentation shall describe how the solution will be implemented, this shall include the following information:

- How the solution is hosted.
- How the solution integrates and shares information with Peace Corps.
- What accounts and permissions are needed for the operations of the solution.
- How automated chatbot interactions function.
- What maintenance and licensing are needed to maintain the operation of the solution.

The design documentation will be used in the Peace Corps change management process to obtain approval for implementation.

3.3.6 Meetings

For all meetings, the Contractor shall be responsible for providing meeting materials and administrative and facilitation support. Meetings will be conducted virtually or through an alternative method of communication (such as teleconferencing), as approved by the Contracting Officer.

3.3.6.1 *Intermittent Project Status Reviews*

At the sole discretion of the Government, intermittent project status reviews may be conducted on an informal basis (by telephone, teleconference, or virtually) upon 3 business days advance notice as approved by the Contracting Officer or other authorized official as COR.

3.3.6.2 *Monthly Project Status Reviews*

Monthly status meetings to be conducted by the 10th of each month. The Contractor is responsible for reporting the previous month's activities (including any risks, issues, or concerns, and actual or recommended actions for their mitigation), and projected activities for the following month.

3.3.6.3 *Program Management Review*

The Government will conduct monthly, quarterly, etc., program management virtual reviews to review the progress of the program, identify any risks, issues, or concerns, and provide feedback on the Contractor's progress and performance. The Contractor shall provide written data and verbal presentations as to the overall status of the VRS Communications Service services, any identified any risks, issues, or concerns (and the mitigation or its plans for the mitigation.]

3.4 SECURITY AND DATA PROTECTION TASKS

3.4.1 Data Protection Plan

The Contractor shall provide a comprehensive Data Protection Plan that outlines how data will be protected throughout its lifecycle. This plan should include details on data encryption (in transit and at rest), access controls, data retention and deletion policies, incident response procedures, compliance with relevant data protection regulations, and data backup and recovery strategies. The Data Protection Plan must be submitted within 15 days of the start of the period of performance and updated as necessary throughout the contract period.

3.4.2 Security Assessment Support

The Contractor shall provide necessary support for government-conducted security assessments. This includes providing required documentation and being available as needed to answer security-controlled questions during Peace Corps security assessments. This limited support is required as requested throughout the contract period.

3.4.3 User Safety Rights

The Contractor shall provide technical information pertaining to the Chatbot for any waiver requests related to safety-impacting or rights-impacting AI tools. The technical information is to be received within 15 calendar days of the request.

3.5 INTEGRATION AND IMPLEMENTATION TASKS

3.5.1 Integration Plan and Report

The Contractor shall develop an Integration Plan detailing how The Chatbot will be integrated with the agency's propriety dataset and the peacecorps.gov website. Following the successful integration, a report documenting the process, challenges, and outcomes must be delivered within 15 days of the integration.

3.5.2 Implementation Plan

The Contractor shall document how the proposed services will be implemented for review and acceptance, including timelines, affected Peace Corps systems, resource requirements, and backout plans. This plan must be submitted 45 days before the scheduled implementation date and will be used in the Peace Corps change management process to obtain approval for implementation.

The implementation plan will be used in the Peace Corps change management process to obtain approval for implementation.

The implementation plan can be incremental to implement functionality progressively.

3.5.3 Test Plan & Results

The Contractor shall provide a testing plan that documents how the proposed solution will be tested for review and acceptance prior to testing. This plan must be submitted 30 days prior to the scheduled start of testing. The Contractor shall also provide the final successful results of UAT testing within 10 days after the completion of UAT testing prior to implementation.

3.5.4 Usability Testing Report

The Contractor shall conduct usability testing with representative user groups and deliver a comprehensive Usability Testing Report. This report should include feedback analysis, compliance with accessibility standards, and recommendations for improvements. The report is due within 15 days after the final design documentation is delivered.

3.5.5 User Acceptance Testing (UAT)

The Contractor shall conduct User Acceptance Testing (UAT) with Peace Corps staff to ensure that the Chatbot meets all functional and non-functional requirements as specified. The UAT must be completed within 30 days following the delivery of the final document documentation. The results of UAT must be documented and delivered in a Test Results report within 10 days after the completion of UAT.

3.5.6 Transparency and Accountability

The Contractor shall develop and maintain documentation of decision-making processes must be maintained and made accessible to authorized personnel to support transparency and accountability.

3.6 DEPLOYMENT TASKS

3.6.1 Final Communication Services Solution

The Contractor shall deploy the final, fully functional chatbot, integrated and tested, across all intended platforms. This final solution must be delivered within 60 days of the successful completion of the final document documentation, testing and cybersecurity risk management and assessment phases.

3.6.2 Training Materials and Knowledge Transfer

The Contractor shall provide comprehensive training materials, including user manuals, training guides, and video tutorials. A training session must be conducted for agency staff, and all materials must be delivered within 10 days before the Chatbot goes live.

4.0 DELIVERABLES

4.1 PRIME DELIVERABLES

The Contractor shall deliver the following functionality to satisfy the objective of this PWS.

4.1.1 Chatbot

The Contractor shall provide an AI chatbot that meets the performance requirements described in

the Two-Way Communication Service Solution Requirements and the Chatbot Solution Requirements sections of this PWS.

4.2 GENERAL MANAGEMENT

The Contractor shall provide the following deliverables for all activities to show the status of contract activities and to manage the delivery of the prime deliverables.

4.2.1 Status Report

The Contractor shall provide a status update for all activities under this contract in monthly reports on the 10th of the month with invoice, excluding weekends and holidays, up until release into production/go live. This shall include progress made in the previous month, activities planned for the upcoming month and risks to the project plan and continuing operations.

4.2.1.1 *Contract Reports*

The Contractor shall provide:

- Meeting Minutes 5 business days after the conclusion of meetings.

4.2.1.2 *Final Report*

The Contractor shall provide:

- Final status report within 30 calendar days from the release into production/go live.

4.2.2 Quality Control Plan

The Contractor shall submit a Quality Control Plan (QCP) covering all task areas and deliverables in accordance with this PWS within 15 days after the start of performance and the final QCP for acceptance within 30 days after the start of performance to the COR and the Contracting Officer. The plan shall demonstrate how the Contractor shall ensure quality performance and satisfy the requirements of the PWS.

4.2.3 Project Plan

The Contractor shall provide an initial Project Plan within 15 days after the start of performance for the implementation and operation of the proposed products, including timelines, resource requirements utilization and milestone dates. The project plan shall also allow for the Agency's change management and security review processes.

The Contractor shall maintain and update the project plan to reflect the current status of the contract activities and projected milestone completion dates. Changes to the project plan shall be noted in the Status report deliverable.

4.2.4 Data Protection Plan

The Contractor shall provide a comprehensive Data Protection Plan that outlines how data will be protected throughout its lifecycle. This plan should include details on data encryption (in transit and at rest), access controls, data retention and deletion policies, incident response procedures, compliance with relevant data protection regulations, and data backup and recovery strategies. The Data Protection Plan must be submitted within 15 days of the start of the period of performance and updated as necessary throughout the contract period.

4.2.5 Requirements Specification Document

The Contractor shall deliver a detailed Requirements Specification Document that captures all functional and non-functional requirements for Chatbot services. This document must be reviewed and approved by the agency before the design phase begins. Delivery is expected within 30 days after the kickoff meeting.

4.2.6 Design and Architecture Documentation

The Contractor shall provide a Design and Architecture Document that details the technical design, system architecture, integration points, and data flows for the Chatbot. This document must be delivered within 45 days following the approval of the Requirements Specification Document. The design documentation shall describe how the solution will be implemented, this shall include the following information:

- How the solution is hosted.
- How the solution integrates and shares information with other Peace Corps systems.
- What accounts and permissions are needed for the operations of the solution.
- How automated chatbot interactions function.
- What maintenance and licensing are needed to maintain the operation of the solution.

The design documentation will be used in the Peace Corps change management process to obtain approval for implementation.

4.2.7 Integration Plan and Report

The Contractor shall deliver an Integration Plan detailing how the Chatbot will be integrated with the agency's website. Following the successful integration, a report documenting the process, challenges, and outcomes must be delivered within 15 days of the integration.

4.2.8 Implementation Plan

The Contractor shall document how the proposed solution will be implemented for review and acceptance, including timelines, affected Peace Corps systems, resource requirements, and backout plans. This plan must be submitted 45 days before the scheduled implementation date and will be used in the Peace Corps change management process to obtain approval for implementation.

The implementation plan will be used in the Peace Corps change management process to obtain approval for implementation.

The implementation plan can be incremental to implement functionality progressively.

4.2.9 Test Plan & Results

The Contractor shall provide a testing plan that documents how the proposed solution will be tested for review and acceptance prior to testing. This plan must be submitted 30 days prior to the scheduled start of testing. The Contractor shall also provide the final successful results of UAT testing within 10 days after the completion of UAT testing prior to implementation.

4.2.10 Usability Testing Report

The Contractor shall conduct usability testing with representative user groups and deliver a comprehensive Usability Testing Report. This report should include feedback analysis, compliance with accessibility standards, and recommendations for improvements. The report is due within 15 days after the final prototype is delivered.

4.2.11 User Acceptance Testing (UAT)

The Contractor shall conduct User Acceptance Testing (UAT) with Peace Corps staff to ensure that the Chatbot meets all functional and non-functional requirements as specified. The UAT must be completed within 30 days following the delivery of the final design document. The results of UAT must be documented and delivered in a Test Results report within 10 days after the completion of UAT.

4.2.12 Training Materials and Knowledge Transfer

The Contractor shall provide comprehensive training materials, including user manuals, training guides, and video tutorials. A training session must be conducted for agency staff, and all materials must be delivered within 10 days before the Chatbot goes live.

4.2.13 Final Chatbot Solution

The Contractor shall deliver the final, fully functional chatbot, integrated, tested, and ready for deployment on the Peace Corps' website. This final solution must be delivered within 60 days of the successful completion of the final design document, testing and cybersecurity risk management and assessment phases.

4.2.14 Key Performance Indicators (KPI) Dashboard

The Contractor shall deliver a live dashboard or regular reports that monitor the Chatbot's Key Performance Indicators (KPIs), including user satisfaction, response accuracy, and adoption rates. The first dashboard/report must be delivered within 15 days of the Chatbot going live, with regular updates as specified by the agency.

5.0 PERFORMANCE REQUIREMENTS SUMMARY (PRS)

The Contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective	***Performance Standard***	***Performance Threshold***	***Method of Surveillance***
The Contractor shall provide all required products and services within the specified time requirements	The Contractor provided Hardware and Software Configuration	Contractor meets the specified time requirement 95% of the time	Periodic surveillance by the Contracting Officer Representative (COR) or Government designee

6.0 ADDITIONAL CONTRACTOR REQUIREMENTS:

6.1 CLOUD INFORMATION SYSTEMS – IT SECURITY AND PRIVACY REQUIREMENTS

The Contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for Moderate impact systems (as defined in FIPS PUB 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for **Moderate** impact systems. The FedRAMP baseline controls are based on NIST (National Institute for Standards and Technology) Special Publication 800-53, Revision 5, *"Security and Privacy Controls for Federal Information Systems and Organizations,"* and also include a set of additional controls for use within systems providing cloud services to the Federal Government.

Peace Corps may choose to terminate the contract if the Contractor has its FedRAMP authorization (Joint Authorization Board [JAB] Provisional or Agency) revoked, and the deficiencies are greater than agency risk tolerance thresholds.

6.1.1 Assessment of the System

The Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement throughout the life of the contract. The Level of Effort for the Assessment and Authorization (A&A) is based on the System's FIPS PUB 199 categorization. The Contractor shall create, maintain and update the following documentation in accordance with the Initial Authorization Package Checklist using FedRAMP requirements and templates, which are available at FedRAMP.gov. (See Appendix B for FedRAMP Initial Authorization Checklist.)

Information systems must be assessed by an accredited FedRAMP Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

The Government reserves the right to perform Security Assessment and Penetration Testing (of its instance). If the Government exercises this right, the Contractor shall allow Government employees (or designated third parties) to conduct Security Assessment and Penetration Testing activities to include control reviews in accordance with FedRAMP requirements. Penetration Testing shall be supported by mutually agreed-upon Rules of Engagement (RoE). Review activities include but are not limited to manual penetration testing; automated scanning of operating systems web applications; wireless scanning; network device scanning to include routers, switches, firewalls, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

The Contractor shall provide access to the Federal Government or their designee acting as their agent when requested in order to verify compliance with the requirements for an Information Technology security program. The Contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

Physical Access Considerations – If the Cloud Service Provider (CSP) is operated within an Infrastructure as a Service (IaaS) that is FedRAMP authorized (e.g., AWS), physical access to the physical data center environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the Contractor's implementation as documented in the Security Assessment Report shall be tracked by the Contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before a Peace Corps authorization is issued.

The Contractor shall be responsible for mitigating all security risks found during A&A and continuous monitoring activities. All critical vulnerabilities must be remediated within seven days, high-risk vulnerabilities must be mitigated within 14 days, and all moderate-risk vulnerabilities must be mitigated within 45 days from the date vulnerabilities are formally identified in accordance with Peace Corps policy. The Government will determine the risk rating of vulnerabilities.

6.1.2 Authorization of the System

Peace Corps will leverage the CSP’s (contractor) FedRAMP Assessment and Authorization package to document and assess the customer controls for which Peace Corps has responsibility and issue a Peace Corps ATO for the agency’s instance of the CSP’s Software as a service (SaaS) or Service as a Service (PaaS) offering. The CSP shall work with the Peace Corps to facilitate documentation and assessment of required customer controls, as necessary. The product shall be designated FedRAMP authorized.

Note: CSPs must comply with all FedRAMP Baseline Controls. Additionally, the CSP shall implement Peace Corps provided specific parameter settings as set forth in the Peace Corps Control Tailoring Workbook- Government Furnished Material (GFM) to be provided at the kickoff meeting.

The CSP shall ensure these essential security controls are implemented and operate as intended.

Further, the CSP shall make the proposed system and security architecture of the information system available to the Office of the Chief Information Officer (OCIO) security team of assigned Information Security Officers (ISSOs) and Subject Matter Experts (SME) for review and approval before the commencement of system build (architecture, infrastructure, and code (as applicable)) and/or the start of A&A in support of the Initial Authorization Package and Continuous Monitoring activities.

6.1.3 Reporting and Continuous Monitoring

Maintenance of the FedRAMP Authorization will be through continuous monitoring and periodic audit of the operational controls within the Contractor’s system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables must be updated in agreement with FedRAMP guidelines and submitted to the repository designated by the FedRAMP program.

The submitted deliverables provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the Peace Corps to leverage the service providers' cloud offering to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors shall be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

In compliance with the Peace Corps agency-specific authorization, the Contractors shall, on a monthly basis (when), collaborate with the ISSO team to provide access to the required deliverables to ensure the CSP maintains an appropriate risk posture.

The Contractor shall furnish access to the following deliverables:

- Monthly OS, database, and web application vulnerability scans as specified in the NIST SP 800-53 Control RA-5 parameter in Peace Corps' Control Tailoring Workbook (deliverable shall include raw results and findings shall be included in the POA&M document);
- Monthly Plan of Action and Milestones (POA&M);
- Change requests (as they occur); and
- Incidents (as they occur)

Upon achievement of FedRAMP authorization, the Peace Corps will accept the FedRAMP A&A and continuous monitoring documentation made available on the repository designated by the FedRAMP program in agreement with FedRAMP guidelines to satisfy the continuous monitoring requirement.

6.1.4 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including Subcontractors) supporting the solution. Peace Corps separates the risk levels for personnel working on Federal computer systems as follows:

- Before accessing the Peace Corps network or any Peace Corps IT system, a favorable initial fitness/suitability determination must be granted, and a Tier 1 or higher background investigation must be initiated. There shall be no waivers to this requirement for Peace Corps network and IT system access for Peace Corps employees or Contractors.
- A favorable initial fitness/suitability determination must be granted, and a Tier 2 or higher background investigation must be initiated before access to Personally Identifiable Information (PII)/ Controlled Unclassified Information (CUI)is granted. The authority and access shall be determined by the appropriate Peace Corps Supervisor (for Peace Corps employees) or CO (for contract personnel), the Data Owner, and the System's AO. Each System's AO, with the request of the Peace Corps Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.
- A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the Peace Corps network or IT systems is granted. A waiver may be requested in order to maintain Peace Corps business

operations; however, such requests should be used judiciously and not incur unnecessary risks to Peace Corps.

If final adjudication of a background investigation is unfavorable, Peace Corps network and IT system access must be revoked, and any GFE, including the Peace Corps PIV card, must be retrieved and returned to OS&S.

Peace Corps shall sponsor the investigation when deemed necessary. No access shall be given to Government computer information systems and Government sensitive information without a background investigation being verified or in process. If the results of the background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a monthly report on separated staff beginning 60 days after the execution of the option period.

6.1.5 Sensitive Information Storage

Controlled Unclassified Information, data, and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. The Contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, *"Guidelines for Media Sanitization."* The destruction, purging or clearing of media specific to the CSP will be recorded and supplied upon request of the Government.

6.1.6 Protection of Information

The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The Contractor shall also protect all Government data, equipment, etc., by treating the information in accordance with its Federal Information Security Modernization Act (FISMA) system categorization.

All information about the systems gathered or created under this contract should be considered CUI information. If Contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same FedRAMP requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

6.1.6.1 *Unrestricted Rights to Data*

The Government will retain unrestricted rights to Government data. The Government retains ownership of any user-created/loaded data and applications hosted on the contractor's infrastructure and maintains the right to request full copies of these at any time.

6.1.6.2 *Personally Identifiable Information*

Personally Identifiable Information (PII) is expected to be stored in the CRM. However, the contractor shall assist in preparing a Privacy Threshold Assessment (PTA) to either document that PII is not in scope or determine which categories of information will be stored, processed, or transmitted by the system. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

PII will require the following guidelines to be adhered to.

- The vendor’s information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains or disseminates PII, the Contractor must complete a PIA and provide it to the Peace Corps Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies, and a system of records notice (SORN) must be published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

6.1.6.3 *Data Availability*

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor and shall not be used for any other purpose other than that specified herein. The Contractor shall provide requested data at no additional cost to the Government.

6.1.6.4 *Data Release*

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In the performance of this contract, the Contractor assumes responsibility for the protection of the confidentiality of Government records and shall ensure that all work performed by its SubContractors shall be under the supervision of the Contractor or the Contractor’s responsible employees. Each officer or employee of the Contractor or any of its SubContractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer, or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

The Contractor shall not disclose Customer Data to any Government or third party or access or use Customer Data, except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would violate a court order or other legal requirement, the Contractor will give the Government reasonable notice of any such legal requirement or order to allow the Government to seek a protective order or other appropriate remedy.

6.1.7 Data Ownership

All Government data collected in the system is the property of the Federal Government. The Contractor (system provider) shall provide all data collected by the system as requested during the contract period and at the completion of the contract period.

6.1.8 Confidentiality and Nondisclosure

Personnel working on any of the described tasks may, at the Government's request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary for the performance of the contract. In the performance of this contract, the Contractor assumes responsibility for the protection of the confidentiality of Government records and shall ensure that all work performed by its SubContractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its SubContractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer, or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

6.1.9 Peace Corps Non-Disclosure Agreement

Each individual Contractor/SubContractor employee who performs work on this contract is required to sign an Employee Non-Disclosure Agreement (NDA). The Contractor shall submit to the COR a completed confidentiality and NDA for each individual Contractor/SubContractor.

The Contractor and all Contractor/SubContractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract and (2) results from or derived from any actual tasks assigned to Contractor employees while participating in this contract is considered proprietary.

The Contractor and all Contractor/SubContractor employees shall not use vendor proprietary information except as necessary to perform this contract and shall agree not to disclose such information to third parties, including any employee of the Contractor/SubContractor who has not executed this NDA or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the Contractor/SubContractor and possible administrative, civil, or criminal penalties.

Note: Peace Corps's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements AOR. Upon request, Peace Corps OGC can advise on NDA development.

6.1.10 Additional Stipulations

Deliverables shall be labeled CUI or Contractor-selected designation per document sensitivity. External transmission/dissemination of CUI to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *"Security Requirements for Cryptographic Modules."*

The Contractor shall certify applications are fully functional and operate correctly as intended on systems using benchmarks from Peace Corps technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the Peace Corps AO. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved benchmark configuration. Information technology for Windows systems should use the Windows Installer Service for installation to the default "program files" directory and should be able to install and uninstall silently. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The Contractor shall use tools to verify their products operate correctly with the approved benchmark configurations and not alter the benchmark settings.

The Contractor shall cooperate in good faith in defining the NDA that other third parties must sign when acting as the Federal government's agent.

Note: Peace Corps' Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements AOR. Upon request, Peace Corps OGC can advise on NDA development.

The Contractor shall comply with any additional FedRAMP privacy requirements.

The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the designated FedRAMP portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. The Contractor shall provide logical access to support incident investigations in accordance with defined FedRAMP Incident Response procedures and/or Peace Corps Incident Response services, which shall be provided as soon as possible but not longer than 72 hours after request.

b. Physical Access Considerations—If the SaaS provider operates within an IaaS that is FedRAMP authorized (e.g., AWS), physical access to the physical data center environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

c. The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Automated scans can be performed by Government personnel or agents acting on behalf of the Government, using Government-operated equipment and Government-specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided in full to the Government.

d. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

The Contractor shall comply with Section 1634 of **Public Law 115-91** that prohibits the use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

The Contractor shall comply with 52.204-25 of the Federal Acquisition Regulation (FAR). It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), Contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), Contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

6.2 SYSTEM ACCESSIBILITY AND EASE OF USE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall comply with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

The Contractor shall comply with the following technical standards as applicable:

- 1194.21 Software applications and operating systems
- 1194.22 Web-based intranet and internet information and applications
- 1194.23 Telecommunications products
- 1194.24 Video and multimedia products
- 1194.25 Self-contained, closed products
- 1194.26 Desktop and portable computers
- 1194.31 Functional Performance Criteria
- 1194.41 Information, Documentation, and Support

The competitor's response must indicate where full details of compliance can be found (e.g., vendor's website or other exact location).

6.3 LOCATION OF PERFORMANCE

All work by the Contractor is expected to be off-site.

6.4 TRAVEL

No travel by the Contractor is expected and shall not be reimbursed.