6Graphical user interface, text, application

Description automatically generated

**Stealth Solutions, Inc.   
Response  
to   
U.S. Department of Homeland Security (DHS)**

**For  
Low Code Application Platform Requirements**

**Request for Information (RFI)**

**December 19, 2024**

|  |  |
| --- | --- |
| Submitted electronically via eBuy to:  U.S. Department of Homeland Security Office of the Chief Information Officer | Submitted by:  Raj Shekhar Vice President, Head of Business Development  46191 Westlake Dr. #112  Sterling, VA. 20165 |

Table of Contents

[A Capability Statement 1](#_Toc185493448)

[B Response to Questions 2](#_Toc185493449)

# Capability Statement

Stealth Solutions, Inc. is a certified 8(a) small business established in 2014 and headquartered in Sterling, Virginia. Our team of highly skilled professionals specializes in delivering comprehensive IT solutions, with a primary focus on innovative low-code/no-code platforms, case management systems, and cloud-based application development. We empower government agencies to achieve operational efficiencies through advanced technology and innovative practices.

Stealth is a recognized leader in implementing Salesforce-based solutions, leveraging our expertise in Salesforce Government Cloud to develop secure, scalable, and user-centric applications. Our proficiency extends to Agile development methodologies, user experience (UX) strategies, DevOps engineering, and cloud migration, ensuring we deliver tailored solutions that align with Federal standards, including FedRAMP, Section 508, and USWDS.

As a trusted partner to Federal agencies like USAID and the Department of Commerce, Stealth excels in delivering mission-critical systems that drive efficiency, transparency, and data integrity. We take pride in our ability to meet diverse client needs while maintaining a steadfast commitment to innovation, security, and quality.

**Past Performance – USAID: Bureau for Humanitarian Assistance (BHA) Hiring and Management System Implementation (CHAMPS)**

1. **Customer Name:** United States Agency for International Development (USAID)
2. **Customer/Client POC Email:** Yvonne Wilson, ywilson@usaid.gov
3. **Total Contract Value:** $4,178,890.42
4. **Period of Performance:** September 2023 – March 2026
5. **Brief Description of Services Provided:**  
   Stealth Solutions is implementing the Contract Hiring and Management Processing System (CHAMPS) within the Salesforce Government Cloud Plus, addressing USAID's critical need for an IT system to manage personal service contractors (PSCs). The CHAMPS application provides:

* Centralized and standardized data governance, reporting, and management.
* Enhanced data quality through error-free data collection and standardized structures.
* Streamlined workflows for hiring mechanisms.
* Robust data security through system-level protocols and role-based access controls.
* Improved decision-making via advanced reporting tools.

Key project deliverables include program management, discovery and needs analysis, solution architecture, data migration, and comprehensive training to ensure seamless user adoption. By automating workflows and enhancing transparency, CHAMPS supports USAID’s mission of reducing the vacancy rate and improving operational efficiency.

1. **Indicate if there is a CPARS Available:** Yes

# Response to Questions

1. Are there any special Terms and Conditions (T&C) the Government should include in any future solicitations, Purchase Orders (POs), or Task Orders (TOs)?

Government solicitations for low-code projects should include T&Cs that ensure data ownership, licensing clarity, and security compliance. The government must retain full ownership of data, with unrestricted access and exportability, while customizations developed are to remain government property. Vendors must comply with standards like NIST 800-53, FISMA, and FedRAMP, ensure platform interoperability with existing systems, and provide detailed documentation for sustainability. SLAs should define performance benchmarks, uptime, and penalties for non-compliance. Accessibility (Section 508), scalability, and innovation should be prioritized, alongside clear exit strategies for seamless transitions, including data migration and training. Transparent pricing, change management protocols, regular audits, and defined dispute resolution mechanisms aligning with Federal Acquisition Regulations (FAR) are also essential for successful long-term implementation.

2. What operational information does the Government need to provide to support accurate proposals (e.g., cost, performance, schedule) for any future solicitations?

To support accurate proposals for future solicitations, the Government should provide detailed operational information, including the project scope, objectives, and specific requirements such as data security, compliance standards, and integration needs with existing systems. Clear timelines, expected deliverables, and performance benchmarks are essential for accurate scheduling and resource planning. Additionally, the Government should disclose available infrastructure, existing tools, and platforms to assess compatibility and customization needs. Historical data on similar projects, anticipated user volumes, and budget constraints will help vendors estimate costs and performance metrics. Transparent communication of priorities, constraints, and risk factors will further enable vendors to craft precise and realistic proposals.

3. What technical information does the Government need to provide to support accurate proposals (e.g., cost, performance, schedule) for any future solicitations?

To support accurate proposals, the Government should provide comprehensive technical information, including system architecture requirements, existing technology stacks, and integration requirements with legacy systems or third-party platforms. Detailed specifications on data storage, security, and compliance needs, such as adherence to NIST, FISMA, or FedRAMP standards, are essential. The Government should also outline performance expectations, such as scalability, uptime, and transaction volumes, alongside any anticipated technical challenges or constraints. Documentation of APIs, data formats, and interoperability standards will aid in assessing customization and development efforts. Additionally, sharing user demographics, accessibility requirements (e.g., Section 508), and planned system usage scenarios will enable vendors to create accurate cost, performance, and schedule estimates.

4. What criteria should the Government use when evaluating and selecting the cloud Low Code Application Platform (LCAP) software?

When evaluating and selecting a cloud Low Code Application Platform (LCAP), the Government should prioritize criteria such as scalability, security, and compliance with federal standards like NIST, FISMA, and FedRAMP. The platform’s ease of integration with existing systems, support for open standards, and robust API capabilities should be assessed to ensure interoperability. Additionally, the platform must demonstrate strong user-friendly features, including intuitive interfaces, accessibility compliance (Section 508), and effective support for both technical and non-technical users. Performance metrics such as uptime, reliability, and responsiveness, along with cost-effectiveness and transparent licensing models, should also be key factors. Finally, the Government should evaluate vendor support, including training, documentation, and long-term maintenance services, as well as the platform's ability to accommodate future growth and innovation.

5. What criteria should the Government use when evaluating and selecting the software Low Code Application Platform (LCAP) software?

Basically a duplicate question from the previous.

6. What performance or Service Level Agreements (SLAs) are important when evaluating and selecting the Low Code Application Platform (LCAP) software?

When evaluating a Low Code Application Platform (LCAP), critical SLAs include uptime and availability, with a minimum threshold of 99.9% or higher to ensure reliability. Performance metrics such as response time and latency should meet defined thresholds under both normal and peak usage conditions. Scalability is essential, requiring assurances that the platform can handle increased user loads and data volumes without performance degradation. Disaster recovery SLAs should specify recovery time objectives (RTOs) and recovery point objectives (RPOs) to ensure swift recovery from outages. Additional considerations include platform security, regular updates to address vulnerabilities, and defined support response times to resolve issues promptly. These SLAs collectively ensure the platform's reliability, performance, and ability to meet government operational needs.

7. If the cloud Low Code Application Platform (LCAP) software uses a mobile device, what mobile devices are supported?

Salesforce, as a cloud Low Code Application Platform (LCAP), supports a wide range of mobile devices through its Salesforce Mobile App, which is compatible with both iOS and Android platforms. It is designed to work seamlessly on smartphones and tablets running iOS 13.0 or later and Android 8.0 (Oreo) or later, ensuring broad device compatibility. The platform provides a responsive and adaptive user interface optimized for various screen sizes and resolutions. Additionally, Salesforce supports browser-based mobile access, allowing users to access key features without the app on mobile devices with modern browsers. This ensures flexibility and accessibility for government operations across diverse mobile environments.

8. If the cloud Low Code Application Platform (LCAP) software uses a web browser, what web browsers are supported?

Salesforce, as a cloud Low Code Application Platform (LCAP), supports all major web browsers, ensuring accessibility across different systems. Recommended and officially supported browsers include the latest versions of Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium-based), and Apple Safari. Salesforce also supports browsers on both desktop and mobile platforms, provided they are modern and HTML5-compliant. For optimal performance, Salesforce advises keeping browsers updated to their latest versions to ensure compatibility with platform features, security updates, and new functionalities. This broad support ensures flexibility for government users across various devices and operating systems.

9. Are there any technical requirements that are specific to a particular software publisher?

Salesforce, as a cloud-based Low Code Application Platform (LCAP), has specific technical requirements to ensure optimal functionality and performance. Users must have a stable internet connection and access to supported web browsers such as the latest versions of Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium-based), or Safari. For mobile access, the Salesforce Mobile App requires devices running iOS 13.0 or later or Android 8.0 (Oreo) or later. Additionally, Salesforce recommends enabling JavaScript, cookies, and TLS 1.2 or higher in the browser settings for secure and seamless access. Integration with other systems may require compatible APIs and connectors provided by Salesforce or third-party vendors. Keeping software up to date and adhering to Salesforce’s guidelines ensures smooth operation and compatibility across environments.

10. How should the attached technical requirements be updated/changed?

To update technical requirements for a Salesforce-based solution, ensure alignment with modern standards for security, accessibility (e.g., Section 508 compliance), and performance, including support for TLS 1.3 and OAuth 2.0. Update device and browser compatibility to include the latest versions of iOS, Android, and modern browsers like Chrome, Firefox, Edge, and Safari. Specify requirements for scalability to handle increasing user loads and data volumes without performance degradation. Emphasize Salesforce’s API capabilities for seamless integration with third-party systems using open standards like REST or SOAP. Strengthen security by leveraging Salesforce’s built-in encryption, multifactor authentication, and compliance with FedRAMP, FISMA, and NIST. Ensure the platform supports Salesforce’s low-code/no-code customization features and provides a user-friendly interface for diverse users. Lastly, require vendor-provided training, a clear roadmap for updates, and support for emerging technologies like AI/ML to future-proof the solution.