# 1 Cover Page

## Stealth Solutions, Inc.
## Response
## to
## U.S. Department of Education
## Office of Career, Technical, and Adult Education Division of Adult Education and Literacy
## for
## Workforce Innovation and Opportunity Act (WIOA) State Plan Portal System
## Request for Information (RFI)

**November 29, 2022**

Submitted electronically via email to:

Contacting Officer: Pamela.Bone@ed.gov
Contract Specialist: Matthew.Lucas@ed.gov

Submitted by:

**Stealth Solutions, Inc.**
Unique Entity Identifier (UEID): RCMZNAHAZ7D9
Socioeconomic Status under the NAICS code 541512: Small Disadvantaged Business, SBA certified 8(a)

*Primary Point of Contact:*
Rahul Sundrani, President
Stealth Solutions, Inc.
46191 Westlake Dr. #112
Sterling, VA 20165
Telephone: 571-230-5642
Email: Rahul.sundrani@stealth-us.com

## 2 Substantive Content

Stealth Solutions, Inc. (Stealth) is pleased to introduce our team for this RFI response. Team Stealth is led by Stealth Solutions, an awardee of the GSA MAS and 8a STARS III contract vehicles. Stealth is a Virginia-based SBA-certified 8a small business incorporated in 2014. Stealth's overall corporate capabilities are Cloud Implementation & Support, Website Development (Drupal) & Support Services, Grants Management Systems Implementation, Business Process Assessment, and Technical Project Management. Our core experience is assisting Federal, State, and local government agencies to achieve performance and operational efficiencies. We achieve proficiencies by optimizing business processes, migrating to, and implementing Cloud solutions, and consolidating and integrating legacy systems to provide a 360-degree view of information on a highly secured Cloud, accessible from everywhere via any web-enabled device.

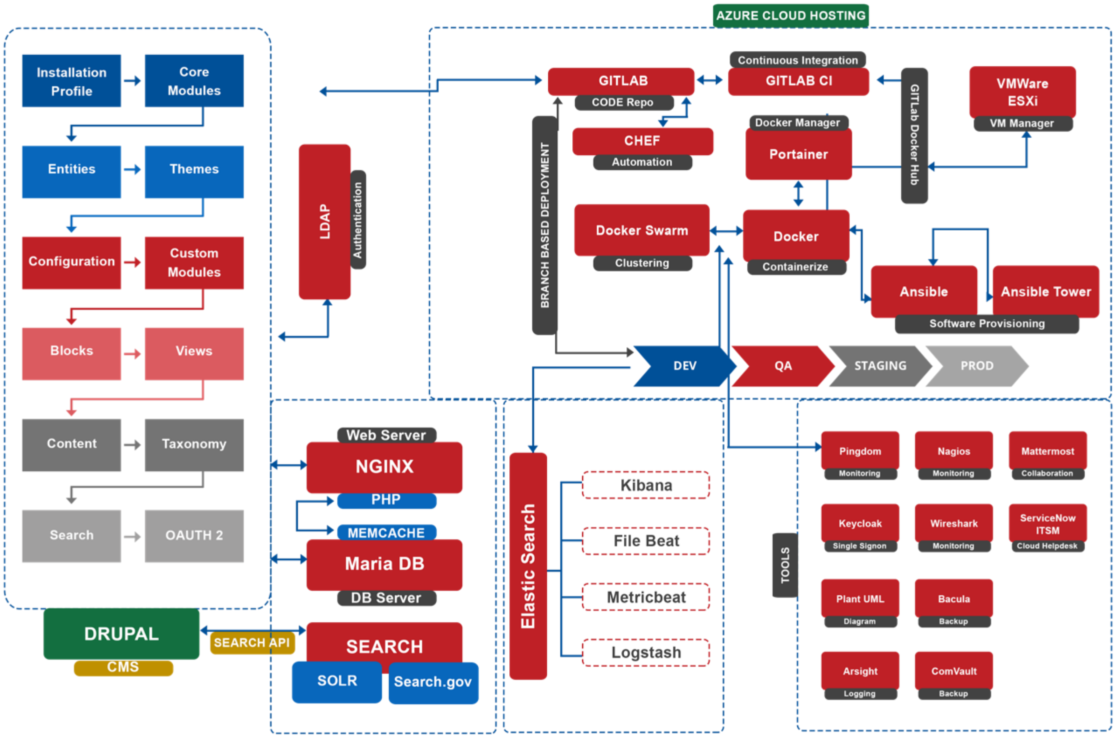
Our contributing subcontractor – teammate, Bravent Systems, is a premiere Web Development and Support Services provider for enterprise-level implementations. Bravent's core expertise is Drupal, open-source technology, Microsoft solutions, and DevSecOps.

Team Stealth has prime and subcontracts awards for the existing Web Support and Development Services at the Department of Commerce, where they support more than 20 websites using Drupal and SharePoint with the NTIA, OCIO, Economic Development Authority (EDA), and Minority Business Development Authority (MBDA).

### Demonstrated Experience Developing in Drupal

Team Stealth has deep expertise in developing and supporting Drupal sites, including configuring core modules; developing custom modules, taxonomy, blocks, views; and migrating content. Team Stealth's approach integrates development and operations into a single-minded entity with common goals: reliable, high-quality software; increased all-around security posture; increased collaboration; faster and efficient releases; and improved customer satisfaction. Key practices developed by Team Stealth have helped government agencies innovate faster by automating and streamlining the software development and infrastructure management processes. Our objective for the Workforce Innovation and Opportunity Act (WIOA) State Plan Portal is to apply these key practices to build an increased security-based website that is primarily reliable and easy to navigate, search, and manage, along with attributes such as Agile Development, Continuous Integration, Continuous Delivery, and Continuous Testing.

The following exhibit shows the components of the system architecture for the Drupal Content Management System (CMS) implementation at the Department of Commerce.



Team Stealth is part of the current team maintaining the Commerce.gov suite of Drupal 9 websites. Therefore, we are well-equipped to develop, maintain, and enhance the WIOA State Plan Portal. Team Stealth has broad experience integrating Drupal for a wide variety of Department of Commerce systems such as Commerce.gov, MBDA.gov, and other Agency systems like GSA.gov, USA.gov, Acquisition.gov, etc. This experience, combined with our knowledge of Drupal architecture and the ecosystem of community-supported plugins enables us to efficiently build new systems and add services to existing applications. Team Stealth has extensive experience creating and customizing Drupal modules. The following are examples of modules created or customized by our Team:

- Drupal SharePoint Integration
- GSA MAX Single-Sign-On
- Advanced Analytics and Charts Integration
- Drupal Salesforce API Integration
- NOAA ICAM Single-Sign-On Integration
- Data.gov API Integration
- Google Login Services Single-Sign-On
- Advanced Custom Workflow
- Accessibility Assessment

Team Stealth has also been involved in several **Drupal migration projects** for federal agencies and has strong experience in designing migration strategies for websites in multiple different technology stacks to Drupal.

Team Stealth fully embraces Agile as our primary method for software development. Our Agile team roles typically include: 1) Architects to implement and adapt compliant system architectures based on proven system design principles; 2) Scrum Masters who ensure the proper implementation and execution of Agile processes; 3) Software Developers and Subject Matter Experts who maintain expertise in relevant technologies including Drupal CMS, and CI/CD toolsets; 4) Systems Engineers who effectively derive requirements and translate business needs into user stories for the product backlog; and 5) Test Engineers with expertise in Section 508 and automated testing tools/methods.

The following table lists URLs of recent project implementations supported by Team Stealth.

| URL | Project |
|---|---|
| https://www.commerce.gov | The main website of the Department of Commerce (built with Drupal 8) |
| www.ntia.gov | NTIA's main public website |
| https://www.Mbda.gov | Minority Business Development Agency's website |
| https://ocio.commerce.gov | Office of the Chief Information Officer, Dept of Commerce website |
| https://ogc.commerce.gov | Office of the General Counsel, Dept of Commerce website |
| https://socmed.commerce.gov | Social Media Tracker |
| https://acetool.commerce.gov | Assess Costs Everywhere (ACE) provides manufacturers with the top reasons for investing and sourcing in the United States. |
| https://citrb.commerce.gov | Department of Commerce IT Review Board |
| https://connection.commerce.gov | Intranet site |
| https://enterpriseservices.commerce.gov | Enterprise Services, Dept of Commerce website |
| https://pass.commerce.gov | Intranet site which provides a single sign mechanism for all Department of Commerce websites |
| https://staff.commerce.gov | Staff Directory website |
| https://www.gsa.gov/ | Central GSA mothership site with access to all of the GSA's resources. |
| https://www.acquisition.gov/ | Federal government's only resource for everything acquisition. |
| https://digitaldashboard.gov/ | One-of-a-kind website scanning every .gov website in the Federal government and collecting compliance information like HTTPS compliance, DAP compliance, IPv6 compliance, Accessibility Compliance (section508) checker, Mobile Compliance checker, etc. |
| https://www.section508.gov/ | Federal government's central website containing accessibility guidelines |
| https://app.buyaccessible.gov/ | A complex website guiding government vendors helps determine if accessibility (Section 508) requirements apply when you purchase Information and Communication Technology (ICT) products and services. |
| https://www.idmanagement.gov/ | Federal enterprise identity playbooks to implement best practices in securing and protecting federal information systems. |
| https://www.navyfederal.org/ | Navy Federal Credit Union, Content and Document Management Sites |
| https://www.usaid.gov/prosperafrica | USAID Prosper Africa Program Web Portal Development and Support Services |
| https://www.eda.gov/ | US Economic Development Administration website |

## Experience with FedRAMP Cloud Service Providers and Federal Cybersecurity Requirements

Team Stealth is well versed with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and pertinent federal agency requirements, standards, guidelines, and procedures for the security of information systems. We have experience with USAID, DOC, NTIA, etc., managing organizational risk using NIST's Risk Management Framework (RMF). We are acquainted with National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5. We understand the WIOA State Plan Portal has already acquired an ATO. However, a continuous security assessment and updates to controls are required as the system is continuously enhanced. Additionally, agencies require that 1/3rd of controls be tested annually. At USAID, for the Prosper Africa Project, Stealth took the transition from the incumbent and worked with M/CIO/IA Compliance and Risk Management (CRM) Team in **acquiring and maintaining an ATO**.

Our approach is to determine the security categorization of the information systems as per Federal Information Processing Standards (FIPS 199). Based on the security categorization, we will select, implement, and maintain all applicable security controls to determine the current state of residual risks, if any. We will ensure timely reporting of security incidents as per NIST and OMB guidelines and will provide incident information as per the established Service Level Agreements (SLAs). The following tasks will be performed by Team Stealth to ensure that all required compliances are met:

- Thoroughly review Agency policies and standards and draft a list of action items that need to be performed either once or regularly to ensure compliance;
- Share the developed plan with the Agency and ensure that we meet all compliance and confidentiality agreements as per FIPS 199;
- Build a continuous improvement review process to ensure that information is protected, and systems are secure;
- Create a detailed plan to develop and maintain security documentation such as System Security Plans (SSPs), Plan of Action and Milestone (POAM), Contingency Plan, Incident Response Plan, etc.;
- Review audit logs, perform security audits, monitor event logs, and conduct disaster recovery testing as required;
- Ensure the system is thoroughly designed and tested to handle PII data and any PII-related incidents; and
- Ensure all resources have completed the necessary and mandatory security training periodically.

In addition to the above, Stealth takes the following pro-active measures to ensure compliance.

### *Development*

Team Stealth ensures that our Development Team follows secure coding practices and integrates security into the design, architecture, and implementation. We have application security touchpoints during the entire lifecycle of development to ensure security is built into the application from the ground up and security impact assessments are performed when there are any changes made to the application and its configuration. We continuously use internal security and vulnerability tools to assess security flaws, and we engage with a third party to evaluate security to further strengthen the system.

### *Testing*

Team Stealth knows that successfully testing an application for security vulnerabilities is of paramount importance. This requires a combination of testing methods to ensure that security flaws that cannot be identified by one method are caught by another method. As such, we utilize a combination of methods such as manual inspections and static code review, threat modeling, and dynamic web application testing. We track all the security flaws found as defects and ensure that these are addressed, and the vulnerabilities mitigated. The WIOA State Plan Portal will be continuously tested for security vulnerabilities with the help of internal and third-party tools such as PMD, CheckMarx, and Net sparker to ensure no security flaws and weaknesses. The vulnerability assessment and mitigation strategies are shared with the agency security staff.

### *Operations*

Team Stealth protects customer data by ensuring that only authorized users have access. Administrators assign data security rules that determine which data users can access. All data is encrypted in transfer, and all access is governed by strict role-based access policies. Team Stealth will comply with protecting Personally Identifiable Information (PII) data in accordance with Moderate to High FISMA/FedRAMP designation. We will follow the guidance in the NIST SP 800-122 "Guide to Protecting the Confidentiality of PII" to protect PII data. Team Stealth will also provide any technical and functional artifacts, including custom code/config created during the project implementation. Additionally, we provide the assurance that all assigned employees will get risk clearances (background checks) by the U.S. Department of Education and obtain government email addresses and PIV cards which are required to access the WIOA State Plan Portal. Additionally, both individually and corporately, all individuals working for Stealth on the project will sign Non-Disclosure and Conflict of Interest Agreements.

To summarize, by leveraging a secure platform, development, testing, and operations approach, Team Stealth will ensure that the WIOA State Plan Portal continues to meet the current and emerging FISMA, FIPS, FedRAMP, and NIST Special Publications system security requirements to stay compliant with the U.S. Department of Education security requirements.

## Experience Working with Federal Grant Projects

Team Stealth has been working with the Grants Management space since its inception. Our staff has experience implementing and supporting Grants Management Systems for federal agencies such as the Federal Emergency Management Agency (FEMA), the Department of Energy (DOE), and the United States Agency for International Development (USAID). Further, in the last few years, we have partnered with REI Systems, Inc. in supporting the implementation of REI's grants management solution, GovGrants®, that serves grants management needs for federal, state, and local government entities as well as leading non-profit organizations, such as the National Endowment for Democracy (NED), Legal Services Corporation (LSC), and the Los Angeles Homeless Services Authority (LAHSA).

GovGrants powered by REI Systems

GovGrants is a cloud-based, low-code, Federal Integrated Business Framework (FIBF)-ready, role-based, fully modular, highly configurable, and highly secure grants management platform. It provides web-based portals for Grantor (Department of Education) staff as well as applicants and grantees to manage grants from opportunity announcement through proposal receipt, review, approval, grant award management, oversight, amendments, and grant closeout. Stealth has implemented GovGrants for numerous federal, state, and local government customers and leading non-profits. The following table provides insights for a couple sample GMS projects.

| LAHSA and NED Grants Management System | |
|---|---|
| Contractor: | Stealth Solutions, Inc. |
| Prime Contractor: | REI Systems, Inc. |
| Project Location(s) [City, State or Country]: | NED – Washington, D.C.<br>LAHSA – Los Angeles, California |
| Project Dollars: | $1,600,000 |
| Contract Type (i.e., FFP, T&M, etc.): | T&M |
| Type of Award (i.e., competitive, sole source, 8(a), etc.): | Competitive |
| Period of Performance: | 05/20 – 12/22 |

Stealth provided the full set of implementation and project management services and delivered a cloud-based Grants Management System to improve and streamline grants processes for the Los Angeles Homeless Services Authority (LAHSA) and National Endowment for Democracy (NED) and improve the experience for their staffs and grantees.

LAHSA

The project included supporting the integration, implementation, and testing of multiple applications on the Salesforce platform. The applications included Case Management, Customer Relationship Management, Grants Management, and e-signature. Stealth Solutions' key responsibilities included the design and development of the solution and testing for quality assurance of the integrated developed solution. This required expertise in project management, integrated software testing, and user interface testing with quality assurance.

NED

Stealth assisted NED in moving from its legacy system to a Salesforce Grants Management System (GMS). Stealth supported various aspects of NED's design, configuration, customization, and testing of the new grants management system. This included working with NED to optimize their grants management processes, including workflows, fields/forms, controls, alerts/notifications, document templates, and user dashboards. In addition, Stealth worked with NED to set up a Grantee Portal that allowed for different grantee touchpoints, including application submission, payment submission, reporting, and monitoring, including narrative and financial reports.

Since its launch, the modern GMS has become a mission-critical system for LAHSA and NED and is used by more than 400 employees and 4,000 grantee users. The modern GMS systems have changed how the government and its grantees interact and manage grants. They no longer work in silos and have transitioned to a workflow-based system that facilitates automation, collaboration, decision-making, and information exchange using features such as its interactive user interface, easy-to-use forms, search capability, collab feature, report generation, and interactive dashboards.

# 3 Vendor Questions

*(1) What, if any, additional information should the Department provide in the PWS to enable you to accurately estimate the price/cost of each task?*

Answers to the following question areas will be helpful in pricing the effort:

- Details on the incumbent and the team composition;
- Award type anticipated (FFP or T&M);
- Number of incumbent staff working on the project and their roles;
- Anticipated number of resources and types;
- Assuming the incumbent has devised a transition plan or have a draft transition plan in place, it will assist for the government to share the transition plan;
- Whether the scope includes any migration (from one Drupal version to another);
- Details on Drupal modules currently used (i.e., how many modules are customized versus those "As Is");
- Additional detail on the extent of customization;
- When the site was last assessed for 508 compliance and the key findings from the assessment;
- Details on security assessment findings and open POA&M;
- Roadmap/functionality to be implemented during the period of performance;
- Type of support required post implementation;
- Sunset of legacy systems requirements
- Integration requirements with external systems; and,
- Details of deliverables by phase and MVP requirements.

*(2) Can you identify any barriers to competition? If so, please identify and describe how the Department could reduce or eliminate those barriers.*

The general barriers to competition for small businesses are based upon a department's willingness to compete the opportunity on a GWAC contract vehicle that is held by an extensive list of small businesses and/or listed as a small business set-aside. This is best accomplished by a small business set-aside on the MAS vehicle or even better is to release the solicitation on the 8(a) Streamlined Technology Acquisition Resource for Services (STARS) III vehicle that currently has more than 1,100 qualified small business contractors. This STARS III GWAC is a small business set-aside contract that provides flexible access to customized IT solutions from a large, diverse pool of 8(a) industry partners.

*(3) Is there any other information that you wish to convey to the Department?*

We noticed many parallels between the WIOA State Plan Portal and normal Grants Management Lifecycles. The processes of WIOA State Plan submission and review processes are very similar to the Application Intake and Review Process in a Grants Management System. Drupal is primarily a content management system and would require extensive customization to build and maintain grants management processes and workflows. Would the government consider a commercial-off-the-shelf (COTS) GMS product that is cloud-based and is offered on a FedRAMP-certified platform, as these products are easier to configure and continue to evolve to support merging technology and regulations and result in a lower total cost of ownership (TCO)?