Stealth Solution Introduction

Stealth Solutions, Inc. (Stealth) is pleased to introduce our team for this RFI response. Stealth Solutions, is 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.

Experience with FedRAMP Cloud Service Providers and Federal Cybersecurity Requirements

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

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

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

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

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 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. 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. <u>LAHSA</u> 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.