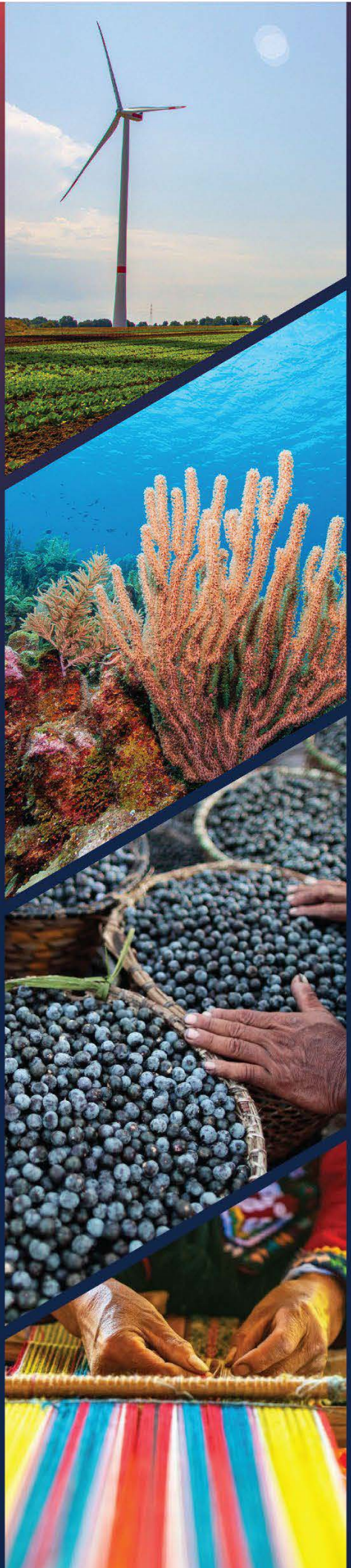

Inter-American Foundation

Grants Management System

Volume IV: Factor III: Security

Solicitation: RFP-IAF-25000-22-0014

Date of Quote: August 25,2022

Submitted to:

U.S. Department of the Treasury
Bureau of the Fiscal Service
Division of Procurement Services

Robert L. Goff, Contracting Officer
Via: purchasing@fiscal.treasury.gov

Submitted by:

REI Systems, Inc.

Kevin M. White, Senior Director of Contracts
14325 Willard Road, Suite 200
Chantilly, VA 20151
Phone: 703.574.9502
Fax: 703.230.0020
kwhite@reisystems.com
www.reisystems.com

UEI: YRNMVN96JC17
CAGE Code: 1DJP1

GSA Contract: 47QTCA19D00DR

Quote Validity: 90 calendar days

TABLE OF CONTENTS

TABLE OF TABLES

VOLUME IV: FACTOR III: SECURITY

1. INFORMATION SECURITY REQUIREMENTS (FACTOR 3) (PWS 8)

Team REI 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 the information systems. We have vast experience in many federal agencies, such as NASA, OMB, DOJ, DOE, HRSA, DHS, and USDA, managing organizational risk using NIST's Risk Management Framework (RMF). Our solution, GovGrants®, is natively designed, deployed, and hosted by the Salesforce.com platform. It will be deployed in Salesforce's Government Cloud Plus environment (FISMA High). Salesforce Government Cloud Plus maintains a Federal Risk and Authorization Management Program (FedRAMP) High Provisional Authority to Operate (P-ATO) from the Joint Authorization Board (JAB), along with comprehensive certifications and compliance attestations such as DoD IL4 PA, IRS 1075, and NIST 800-171.

Team REI will work with IAF 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 and implement all applicable security controls and 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 to IAF as per the established Service Level Agreements (SLA). Compliance documents related to system security control are available at https://compliance.salesforce.com/. Incidents related to security and other issues are posted in real-time on the Salesforce Trust website at https://status.salesforce.com/.

1.1 Federal Information System Security Requirements (8.1)

GovGrants is natively designed, deployed, and hosted by the Salesforce.com platform. Salesforce maintains a formal company-wide Information Security Management System (ISMS) that conforms to the requirements of the ISO 27001 standard, FedRAMP, DoD cloud computing authorization, and the NIST CSF, FIPS, including security policies, standards, and procedures. We ensure that the application meets the current and emerging FISMA, FIPS, FedRAMP, and NIST Special Publications system security requirements for a moderate impact system baseline.

The IAF instance will be deployed in Salesforce's Government Cloud Plus environment. This is a dedicated instance of Salesforce's multi-tenant community cloud infrastructure specifically for use by U.S. federal, state, and local government customers. It has been designed to provide U.S. Government customers with privacy and high levels of performance, reliability, and security. Team REI will work with Salesforce and IAF staff to support activities listed in **Table 1**.

Table 1: Supported Activities

Activities	Documentation
Security Control Assessment and Authorization	Part of the security plan
Continuous Monitoring	Part of the security plan
POA&M mitigation	Part of the security plan and configuration management plan
Audit requirements	Part of the security plan

1.1.1 PWS 8.1.1

GovGrants is natively designed, deployed, and hosted by the Salesforce.com platform. It will be deployed in Salesforce's Government Cloud Plus environment (FISMA High). Salesforce Government Cloud Plus maintains a FedRAMP High P-ATO from the JAB, along with certifications and compliance attestations such as DoD IL4 PA, IRS 1075, and NIST 800-171.

1.1.2 PWS 8.1.2

Salesforce maintains a Continuity of Operations (COOP) and Disaster Recovery (DR) Plan that supports a robust business continuity strategy for the production services and platforms. The Disaster Recovery plan is constantly measured against strict regulatory and governance requirements and is a crucial part of the acceptance plan when making changes or additions to the production environment. Team REI will ensure that the plan meets the Recovery Time Objectives (RTO) and the Recovery Point Objectives (RPO) established after the Business Impact Analysis (BIA) for the IAF application. Details can be found at this site: https://compliance.salesforce.com/en/disaster-recovery-bcp.

1.1.3 PWS 8.1.3

Team REI 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. GovGrants is continuously tested for security vulnerabilities with the help of internal and third-party tools such as PMD, CheckMarx, and Netsparker to ensure that there are no security flaws and weaknesses. The vulnerability assessment and mitigation strategies are shared with the IAF security staff. GovGrants is an AppExchange-certified managed package that must pass the Salesforce Security review. This comprehensive security review identifies coding vulnerabilities that must be mitigated before acceptance of the managed package.

1.1.4 PWS 8.1.4

Salesforce undergoes System and Organization Controls (SOC) 1 examination semi-annually, completes SOC 2 and SOC 3 for Service Organizations audits, and has achieved compliance with PCI-DSS. Salesforce has also obtained ISO 27017 and 27018 certifications.

All certifications will remain in place for the duration of the contract. REI also holds current ISO/IEC 27001:2013 and ISO/IEC 20000:2018 certifications, and we will provide IAF with the compliance certificates to that effect.

1.1.5 PWS 8.1.5

GovGrants will be deployed in Salesforce's Government Cloud Plus environment (FISMA High), which maintains a FedRAMP High P-ATO from the JAB, along with certifications and compliance attestations such as DoD IL4 PA, IRS 1075, and NIST 800-171. We will work with the IAF stakeholders to address, implement, and comply with all applicable management, operational, and technical controls to maintain the ATO status continuously.

1.1.6 PWS 8.1.6

GovGrants leverages the identification and authentication methods provided by Salesforce.com. Salesforce protects customer data by ensuring that only authorized users can access it. In addition to the standard login credentials method, GovGrants also inherits Salesforce Multi-Factor Authentication (MFA) protocols for additional security. GovGrants supports Salesforce

Authenticator, Microsoft Authenticator, Google Authenticator, and Chrome-browser extension Authenticator. Other authenticators can be evaluated and integrated upon request.

1.2 Security and Compliance (PWS 8.2)

1.2.1 PWS 8.2.1

GovGrants uses the Salesforce platform to ensure the confidentiality of sensitive data. Salesforce leverages advanced technologies and administrative, technical, and physical controls to ensure the security, confidentiality, and availability of Salesforce services. These services include but are not limited to Service availability, architecture and data segregation, security controls, security policies and standards, security audit logs, incident management, user authentication, physical security, reliability and backup, disaster recovery, data encryption, and protection from deletion of customer data.

To protect customer data from unauthorized access, Salesforce provides advanced protections such as Employee Background Investigations, Employee Authentication, Physical Access Controls, Logical Access via Application, and Logical Access via Server.

Team REI has a long track record of developing and hosting secure information systems for many federal agencies, and we understand that security is a critical component of systems and applications. We ensure that our Development Team integrates all security design, architecture, and requirements while developing the code. This includes, among others, integration of the relevant security controls related to Identification & Authentication, Access Controls, Audit & Accountability, Configuration Management, Maintenance, System & Communication Protection, and System & Information Integrity. The solutions are tested on platforms that are hardened per industry standard benchmarks and other security guidance based on the security categorization of the systems. Role-based granular access is built into the applications and databases that encrypt sensitive data using FIPS 140-2 validated cryptographic modules.

As a longstanding provider of IT solutions to the government, REI, an ISO/IEC 27001:2013 and ISO/IEC 20000:2018 certified company, has developed and implemented a robust and comprehensive set of IT security policies and procedures that comply with NIST SP 800-53 and NIST SP 800-171 guidance to protect the confidentiality, integrity, and availability of sensitive information of its customers. We continuously monitor our facilities and networks to prevent unauthorized access to our systems and sensitive information. All our employees undergo background checks and are required to undertake mandatory annual security awareness and insider threat training. Each employee must read, accept, and sign REI's security policies and "Rules of Behavior." We undergo third-party annual surveillance audits for the ISO/IEC 27001:2013 and ISO/IEC 20000:2018 re-certifications.

1.2.2 PWS 8.2.2

Background checks, including criminal record checks, are conducted before hiring any resources at REI. Such verifications are completed by third-party experts. In accordance with the Fair Credit Reporting Act (FCRA), credit checks are performed when required by the contract and for positions with financial responsibilities. This is a common request as many of our federal projects require Public Trust or Secret clearances. We will ensure that all REI employees and subcontractors placed on this contract undergo background investigations as mandated by IAF.

1.2.3 PWS 8.2.3

Team REI will provide IAF with written Corporate Policies and Procedures that will outline our security posture. It will include, among others, integration of the relevant security controls related to Identification & Authentication, Access Controls, Audit & Accountability, Change &

Configuration Management, Maintenance, System & Communication Protection, and System and Information Integrity. The written policies will also include incident response, processes for notifications and remediating unauthorized release of data, site inspections, and security audits.

1.2.4 PWS 8.2.4

GovGrants will be deployed in Salesforce's Government Cloud Plus environment (FISMA High). Salesforce Government Cloud Plus maintains a FedRAMP High P-ATO from the JAB, along with comprehensive certifications and compliance attestations such as DoD IL4 PA, IRS 1075, and NIST 800-171.

1.2.5 PWS 8.2.5

Team REI will comply with protecting Personally Identifiable Information (PII) data in accordance with Moderate to High FISMA/FedRAMP designation. We will follow the guidance contained in the NIST SP 800-122 "Guide to Protecting the Confidentiality of PII" to protect PII data. Salesforce is compliant with ISO 27018 and HIPAA to protect personal information.

We will comply with providing security and software updates using GovGrants framework packages and Salesforce security setup. IAF will have full ownership of all its business data throughout the life of the project and can retrieve it at any time. IAF will also own any technical and functional artifacts, including custom code/config created during the project implementation.

1.2.6 PWS 8.2.6

Team REI's GovGrants solution will comply with FIPS-201, FIPS PUB 199, FIPS PUB 200, NIST SP 800-18, NIST SP 800-37, NIST SP 800-53, NIST SP 800-60, and IAF security policies and procedures, FISMA, and FedRAMP.

1.3 Corrective Actions (PWS 8.3)

Given the dependency of the GovGrants product on the Salesforce platform, Team REI provides Service Level Objectives to all its customers, starting in the production environment. Team REI and Salesforce will respond to outages, downtime, and other issues within 24 hours.

Salesforce typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, they may invite impacted customers to join a conference call about the incident and Salesforce's response. If there is an outage of the Salesforce/GovGrants system, Team REI will escalate it to the Salesforce premier support team as soon as we are aware of it.

All corrective actions that require more than 24 hours will be documented and provided in an email to the COR. We will also provide the COR with a mitigation schedule, milestones, and updates as needed.

1.4 Cloud Service Provider (PWS 8.4)

GovGrants is hosted on the Salesforce.com platform, which is FedRAMP-compliant as per FISMA and NIST guidelines. To maintain the security authorization, Team REI will provide IAF with FedRAMP/FISMA-related documentation. We will also provide description and evidence of the effectiveness of the continuous monitoring program, including security incident response, change management, key management, and escrow services. We will ensure timely reporting of security incidents as per the NIST and OMB guidelines and support IAF to evaluate the implemented security controls before the ATO is granted.

From the system point of view, GovGrants can show the login history of all the users (time, location, IP address, and browser) and help auditors in the audit process if user access is an area of investigation. Setup audit trails are available and store all major system-level activities such as changes in password policies, session settings, etc.

GovGrants offers deep audit trails. All notifications, email exchanges, and assigned tasks are also recorded in the system for later reporting. Special reports can be generated based on the program or audit needs and can be made accessible only to the auditors for verification purposes.

Any infrastructure-related processes are handled by Salesforce as part of their setup. Infrastructure logging is enabled to capture system activity, and logs are forwarded to a central logging system. Events are logged and monitored for anomalies.

1.5 Configuration Management (PWS 8.5)

1.5.1 Configuration Management Plan (PWS 8.5.1)

REI has built the GovGrants product utilizing an integrated quality approach to define quality standards, measure quality, and continuously improve quality. REI used the internal process standards and controls which comply with ISO 9001:2008 and Software Engineering Institute's Capability Maturity Model Integration (CMMI) Development Level 3 processes, standards, and best practices for software development methodology. Testing types include unit testing, functional testing, performance testing, security testing, automation testing, etc. REI will maintain a FISMA-compliant Configuration Management Plan that includes the inventory of the components of the GovGrants system, relevant GovGrants specific baseline configuration settings, relevant Salesforce baseline configuration settings, and their impact on the system. The plan will also consist of changes from the baseline across all the sandbox environments (Dev, QA, UAT) and production environments.

1.5.2 Secure Development (PWS 8.5.2)

Team REI will ensure that our Development Team follows secure coding practices and integrates security into the design, architecture, and implementation. We will have application security touch points 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. Additionally, GovGrants is a certified AppExchange package, which means it goes through a rigorous Salesforce security review process of the entire codebase annually. Issues arising from these are resolved or mitigated during the product development lifecycle before a release is ready to be implemented for a customer.

1.6 Secure Operation (PWS 8.6)

GovGrants is natively built and deployed on the Salesforce.com platform, which is developed with secure software development best practices, much like Open Web Application Security Project (OWASP) web application security. Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define company-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer, and all access is governed by strict role-based access policies. The Salesforce Security Guide describes the various systems and administrative functions that provide security within GovGrants.

The up-to-date Salesforce Security Guide document is available at https://resources.docs.salesforce.com/238/latest/en-us/sfdc/pdf/salesforce_security_impl_guide.pdf.