Recipient Information

To: BID CLERK DEPARTMENT OF ADMINISTRATION PURCHASING
Company: State of West Virginia Purchasing Division
Fax #: 3045583970

fax

Sender Information

From: Nehal Mehta
Company: GEOACL LLC DBA RAINBOW SECURE
Email address: nehal@rainbowsecure.com (from 24.185.56.104)
Phone #: 17327237955
Sent on: Tuesday, March 26 2024 at 8:38 AM EDT

VENDOR NAME: GEOACL LLC DBA RAINBOW SECURE
VENDOR CONTACT: Nehal Mehta nehal@rainbowsecure.com
BUYER: The State of West Virginia Purchasing Division
Larry D McDonnell
304-558-2063 larry.d.mcdonnell@wv.gov
SOLICITATION NO.: CRFP 0947 ERP2400000002
Proc Folder: 1376334
Doc Description: Identity Management Single Sign-On Solution
BID OPENING DATE: 03/26/2024
BID OPENING TIME: 13:30
VENDOR FAX NUMBER: 270-513-9540

VENDOR NAME: GEOACL LLC DBA RAINBOW SECURE

VENDOR CONTACT: Nehal Mehta nehal@rainbowsecure.com

BUYER: The State of West Virginia Purchasing Division

Larry D McDonnell 304-558-2063 larry.d.mcdonnell@wv.gov

SOLICITATION NO.: CRFP 0947 ERP2400000002

Proc Folder: 1376334

Doc Description: Identity Management Single Sign-On Solution

BID OPENING DATE: 03/26/2024

BID OPENING TIME: 13:30

VENDOR FAX NUMBER: 270-513-9540

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder:	1376334		Reason for Modification:
Doc Description:	Identity Management Single Sign-On Solution		
Proc Type:	Central Master Agreement		
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2024-02-23	2024-03-12 13:30	CRFP 0947 ERP2400000002	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name : GEOACL LLC DBA RAINBOW SECURE

Address :

Street : 74 CORONA CT

City : OLD BRIDGE

State : NJ **Country :** UNITED STATES **Zip :** 08857

Principal Contact : NEHAL MEHTA, President and CEO

Vendor Contact Phone: +1732-723-7955 **Extension:**

FOR INFORMATION CONTACT THE BUYER
Larry D McDonnell
304-558-2063
larry.d.mcdonnell@wv.gov

Vendor Signature X N.V. Mehta **FEIN#** 46-3879075 **DATE** 03/25/2024

All offers subject to all terms and conditions contained in this solicitation

MWBE Preference:

GEOACL LLC DBA RAINBOW SECURE is a SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESS.

NJ don't give preference to local MWBE companies.

See Minority and/or Women Business Enterprise (M/WBE) | Business.NJ.gov

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) NEHAL MEHTA

(Address) 74 CORONA CT, OLD BRIDGE NJ 08857

(Phone Number) / (Fax Number) 732-723-7955

(email address) nehal@rainbowsecure.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

GEOACL LLC DBA RAINBOW SECURE
(Company)

N. V. Mehta
(Signature of Authorized Representative)

NEHAL MEHTA, President and CEO 03/25/2024
(Printed Name and Title of Authorized Representative) (Date)

732-723-7955
(Phone Number) (Fax Number)

nehal@rainbowsecure.com
(Email Address)

Proposed Solution:

RAINBOW SECURE SINGLE SIGN-ON running on Cloud using SAML Protocol, authenticating users for SP Service Providers (SaaS Apps, Cloud tenants, Identity platforms and custom applications) that can be integrated with Microsoft Entra, Google ID, Oracle ID, Ping ID, IBM ID, and other Identity providers.

Add-on: RAINBOW SECURE IDENTITY AND ACCESS MANAGEMENT for Cloud Based Identity

Add-on: RAINBOW SECURE MFA (Multi-layer Multi-factor Authentication)

Add-on: RAINBOW SECURE ONE TIME PASSWORD Login

Users get one unified digital identity and seamless login into applications and software services used by State of West Virginia.

What is RAINBOW SECURE SINGLE SIGN-ON? HOW DOES IT WORK?

How It Works:

Rainbow Secure SSO works by establishing a trust relationship between the authentication system and the applications requiring user authentication. When a user logs in to the SSO system, it authenticates their identity and provides a token or assertion that the user is who they claim to be. This token is then used to access other applications without the need for additional logins, streamlining the user experience and enhancing security by reducing the number of times a user needs to enter their credentials.

Why Choose Rainbow Secure SSO?

Rainbow Secure emphasizes eliminating common cyber threats such as keyloggers, brute force attacks, malware, phishing, password reuse, device cloning, and many others. By reducing the reliance on multiple passwords and enhancing the security of the authentication process, Rainbow Secure aims to provide a secure, efficient, and user-friendly authentication solution.

Rainbow Secure's approach to security, including the avoidance of auto password generators and protection against a wide array of cyberattacks, positions it as a robust solution for organizations looking to secure their digital assets while providing a seamless login experience for their users.

Solution Capabilities:

4.3.1.1. Can apps integrate directly with the solution's Application Programming Interface (API) to perform restful Application Programming Interface calls such as reading user information, or making changes to user objects, group membership.

Yes, Rainbow Secure SSO Solution has API for

- reading user objects,
- to manage user life cycle by making changes to user objects and its status
- to read and manage user group membership

4.3.1.2. Indicate if the proposed solution provides the ability to create custom Application Programming Interface access policies and/or authorized servers. Provide details.

Yes, you can create custom access policies.

4.3.1.3. Indicate if your service/solution offers Application Programming Interface token management and creation. If the solution offers this capability, provide details on API token management and creation capabilities.

Rainbow Secure offers API for storing and managing sensitive configuration items including tokens.

4.3.1.4. Describe the Application Programming Interface capabilities your solution offers for integration with custom applications and workflows.

Rainbow Secure SSO offers integration with SaaS, Cloud and IAM user identities using SAML Protocol. For custom applications that cannot use SAML, it offers custom API for SSO login and user identity management.

4.3.1.5. How do you ensure the security and privacy of data transmitted through your Application Programming Interfaces?

Data is encrypted during transit and rest using industry standard protocols and best practices.

4.3.1.6. Can your solution support standards like Open Authorization (OAuth) 2.0 and OpenID Connect for secure Application Programming Interface access?

Rainbow Secure SSO has partner plugins for OAuth 2.0 and OpenID authentications.

4.3.1.7. Detail the scalability of your Application Programming Interface infrastructure

to support high volumes of authentication and authorization requests.

Yes, our APIs for SSO and IAM are highly scalable. Our solution is deployed in reliable public and gov cloud environments that has proven ability to handle 500K plus users.

4.3.1.8. Does your solution provide Remote Authentication Dial-In User Service

(RADIUS) support that does not require on-premise components?

No.

4.3.1.9. Indicate if the solution provides supported push notification. If so, what

controls can be used to lower the risk of push fatigue attacks.

You can use Google Authenticator or any other option for push notification on optional basis. We can configure to not ask again for same IP on same day provided user opts for friendly and interactive Rainbow Secure Password Login that gives multi-layer defense by defeating phishing, stolen credentials replays, brute-force and keylogger malware attacks.

4.3.1.10. List the Multi-factor methods supported.

Rainbow Secure Multi-factor Authentication

Rainbow Secure MFA + Google Authenticator

Rainbow Secure MFA + GEOACL Location fencing

Rainbow Secure MFA + Google Authenticator + GEOACL Location fencing

Rainbow Secure Multi-factor Authentication + Scanned Barcode unique for given location for given date range

Rainbow Secure Multi-factor Authentication + Rainbow Secure Password Login + GEOACL Location fencing

4.3.1.11. Does your service offer out of the box login flows that protect against bruteforce attacks?

Yes, that's our winning point against all other SSO IAM providers. Our out of the box, unique, patented color and font style enabled interactive user authentication process defeats brute-force, phishing, automated BOT and keylogger malware type attacks.

https://www.rainbowsecure.com/mfa-multi-factor-authentication/

https://www.rainbowsecure.com/rainbow-password/

4.3.1.12. Indicate if the proposed service offers out of the box login flows that protect

against brute-force attacks and describe the protection against these attacks.

Yes, it does offer login flows to protect against brute-force attacks out of the box.

4.3.1.13. Detail the authentication methods supported by your platform (e.g., Email, Multi-Factor Authentication (MFA), Short Message/Messaging Service (SMS), MFA, Biometric/Web Authentication API (WebAuthN), and define any other capabilities that the vendor offers.

Yes, Rainbow Secure MFA Supports authentication method given below:

Passwordless / MFA login with OTP over Email, Short Message/Messaging Service (SMS)

Biometric/Web Authentication API (WebAuthN) using partner hardware and API

Passwordless / MFA login with:

OTP over Email, Short Message/Messaging Service (SMS) and formatting instruction over secondary Email, Phone,

OTP over Email and formatting instruction over Phone where formatting instruction is something like make it bold, make it font style 10, color it blue etc...

4.3.1.14. How does your solution provide adaptive authentication based on risk

assessment?

It processes numerous login session attributes and login session history and its results and deciedes to stop or allow further processing of user login (step up) using authentication method custom assigned for given situation.

4.3.1.15. Can your solution integrate with third-party identity providers for federated

authentication?

Yes, it does integrate with 3rd party IDPs such as Microsoft Entry (Azure AD), Google ID, Okta, Ping Identity, Oracle ID, IBM ID etc.

4.3.1.16. Indicate which authentication protocols the proposed solution supports (e.g.,

Security Assertion Markup Language (SAML) 2.0, OpenID Connect (OIDC) ,

Remote Authentication Dial-In User Service (RADIUS). Identify any other

authentication protocols the proposed solution offers.

We support SAML out of the box. We also offer custom APIs for SSO to custom applications that don't use SAML. We have partner plugins for OpenID and RADIUS authentication.

4.3.1.17. Explain how your solution adapts authentication methods based on contextual

factors like location and device.

It easily adapts to change in location, device and date time factors, approves or denies user login.

4.3.1.18. How does your solution handle scenarios where a user has lost their primary

authentication device?

We offer SSO and MFA user authentication options that allows users to use multiple devices for login.

4.3.1.19. Can the solution block access based on blacklisted Internet Protocol (IP) addresses or Geogrpahy (GEO) location?

Yes, it can block access to blacklisted IP and geo-locations.

4.3.1.20. Does the service identify, detect, and block suspicious authentication activity?

Yes.

4.3.1.21. Does the solution perform behavior detection during authentication? (Example: Impossible Travel, Device context, Network Context,)

Yes.

4.3.1.22. How does your platform detect and prevent unauthorized access?

Yes.

4.3.1.23. Can your platform support attribute-based access control (ABAC) to dynamically adjust access based on user attributes?

Yes, it offers ABAC settings to adjust user access at run time.

4.3.1.24. Can your solution integrate with external identity providers to extend authorization capabilities?

Yes, it does integrate with IDP from Microsoft, Google, Oracle, Okta, Ping identity etc.

4.3.1.25. Can your platform enforce access policies based on contextual factors such as, but not limited to time of day, location, and user behavior?

Yes. We offer standard and custom access policies. We offer services to further customize our SSO login workflows to suit your organization's need to connect unique and custom applications where possible by protocol support or availability of custom application developers to consume our custom API for SSO.

4.3.1.26. Describe your solution's approach to enforcing the principle of least privilege for user access.

Configure groups as per organization policy.

4.3.1.27. How does your platform support session termination and re-authentication based on inactivity or specific triggers?

Yes.

4.3.1.28. Does the solution have the ability to have isolated lower environments for the purposes of testing / development?

Yes.

4.3.1.29. Does your solution provide multiple environments for testing purposes?

Yes.

4.3.1.30. Does the solution allow automation of tasks through scripting or Application Programming Interface calls?

Yes.

4.3.1.31. Do you offer flexible application integrations such as general Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and Open Authorization (Oauth) connectors?

Yes, SAML out of the box. OIDC and OAuth using partner plugins.

4.3.1.32. Do you offer deployment assistance, documentation, or training to ensure a smooth transition to your platform?

Yes, we offer services to assess your environment, make a plan for orderly migration of user identities, applications and adjust IAM process.

4.3.1.33. Can the solution leverage Active Directory as the Identity Provider? If so, do agents need to be installed on our systems to facilitate that communication?

Additionally, is your solution capable of syncing that information in real time?

Yes, we have ETL jobs to sync with Azure AD. Yes agent needs to be installed on your systems to sync with Active Directory.

4.3.1.34. If an agent is required to facilitate a connection between Active Directory and your service, please describe how that information is exchanged securely.

Using encrypted communication session and rotating tokens.

Additionally, please describe how redundancy and failover can be configured to ensure there is a constant flow of information.

We monitor each tenant 24/7, have hosting that can failover seamlessly over local or national data centers.

4.3.1.35. Does the solution support the ability to import password hashes from other

Identity Providers (IDPs)? If so, describe what hashing algorithms are

supported and how that process works.

No, we don't import password hashes but offer user to do passwordless login and set new password or original password.

4.3.1.36. Do you have an administrator dashboard User Interface (UI) to manage users?

Yes. We have a dashboard to allow admins to manage users.

Can you enforce a specific multi-factor type for administrative access?

Yes, we can customize multi-factor type by user role.

4.3.1.37. Does the solution support external federation? If so, how, and what Identity

Providers (IdPs) are supported?

Yes, we support external federation using SAML.

4.3.1.38. How does your solution streamline user onboarding and offboarding processes?

We give single pane of glass management for user access management, and offboarding.

4.3.1.39. How does your platform handle role-based access control and user

provisioning?

Admins have ability to create and assign users to groups, assign access to groups and assign users to groups.

4.3.1.40. What customization options are available for the user interface and branding?

You can customize login and admin page headers and footers using your logos, URLs and color schemes.

4.3.1.41. Are all Muti-Factor Authentication (MFA) factors available for use in

authenticating a user prior to performing self-service password maintenance?

Yes.

(E.g., Forgot Password, Change Password, Account Unlock)

4.3.1.42. During a password reset, does the solution compare the supplied new password against a public database of known-compromised credentials and blocked the use of compromised credentials?

Rainbow Secure SSO offers multi-layer password that invalidates millions of compromised credentials available on dark web. For users with legacy type of password credential we can use 3rd party service that offers option to compare and block use of compromised credentials.

Background: Rainbow Secure SSO offers color and style enabled password and OTP login options. Users type in password / OTP and formats the credentials, what you know / have + what you do factor.

4.3.1.43. Describe the self-service features available to end-users for password resets and profile updates.

Users can manage their accounts, resets their account passwords.

4.3.1.44. How does your platform handle de-provisioning of user access when an employee leaves the organization?

When employee leaves the organization, admin can disable the employee access and user will no longer will be able to access any application going forward.

4.3.1.45. What mechanisms are in place to ensure that user access is granted or revoked promptly?

Automation

4.3.1.46. Does your service integrate with third-party logging solutions? If so, what logging formats are supported (i.e. JavaScript Object Notation (JSON), Comma separated Variable (CSV), and define any other capabilities that the vendor offers. And are they sent in real-time?

We use in-house logging as well as offer to export audit log to external databases. Yes, loggin is real-time.

4.3.1.47. Does the solution provide reporting on authentication statistics (Single Sign On (SSO) attempts, Multi-Factor Authentication (MFA) enrollment, new user creation, lockouts, permission changes, password resets), and define any other capabilities that the vendor offers.

Yes, we offer statistics on SSO, MFA, user management, password, permission changes etc.

4.3.1.48. How long are the logs maintained? 3 months. We can maintain longer based on your organization need.

4.3.1.49. Do you provide any ability to create or pull reports? Do you have any templates

for executive type reports?

We provide pull reports. Also offer option to export audit logs and create reports using your own BI environment. We can create custom templates for executive type reports.

4.3.1.50. Please provide the full list of security events and descriptions captured by your

service.

User created, User modified, User disabled, User access changed, User MFA method changed, User Password changed, Suspicious login activity, Login attempt recorded, Successful login, Login failure and others

4.3.1.51. Explain the logging mechanisms in place to capture identity-related events and

activities.

Monitoring of user object changes for user life cycle related changes.

4.3.1.52. How does your solution provide real-time alerts for security incidents and

policy violations?

Email, SMS, Database logging

4.3.1.53. Can your solution meet compliance requirements by generating audit trails and

activity reports?

Yes.

4.3.1.54. What options are available for exporting logs and reports to external systems or

Security information and event management (SIEM) solutions?

Export options for exporting audit logs.

4.3.1.55. Indicate and identify any countries where you provide services to clients

outside of the United States (and US territories).

We offer service only in United States and Canada.

4.3.1.56. Have there been any significant security breaches in the past 24 months? If so

please provide documentation of how this breach occurred, how many accounts

were involved, and the remedy/solution for the breach.

No significant breaches in past 24 months.

4.3.1.57. Provide information on how clients are informed of maintenance and patch releases.

We use change management and inform our clients as per our change communication policy.

4.3.1.58. Where does the solution reside?

In Microsoft Azure Cloud

4.3.1.59. Describe how your service is compliant with Americans with Disabilities Act (ADA) standards and how you support screen readers and descriptive technology.

We support it. We use 3rd party plugin to enable it.

4.3.1.60. Describe how your service provides failover and redundancy.

We use geo redundant hosting, backups, 24/7 monitoring and alerts to maintain reliable SSO, MFA and IAM service.

4.3.1.61. What controls does your service have in place to prevent automated attacks?

Pen testing, AI monitoring, Risk analytics, Cloud Security controls, and admin trainings.

4.3.1.62. How does your solution ensure high availability and resilience in the face of unexpected outages or disasters?

We offer secondary stand by sites on alternate trusted cloud providers. We can discuss more on call.

4.3.1.63. Provide your data backup and recovery strategies to safeguard against data loss?

Backups, Fail safe backup archives.

4.3.1.64. Describe your approach to continuous monitoring and threat detection within your identity infrastructure.

24/7 AI monitoring, service level monitoring, outage monitoring

4.3.1.65. Can your solution provide insights into user behavior anomalies that might indicate compromised accounts?

Yes, We provide valuable risk analytics.

4.3.1.66. How does your platform ensure data integrity and protection against unauthorized modifications of user attributes?

We monitor changes to user attributes, communicate it to user, log the changes in audit log, follow role based access control so only authorized admin user can make changes.

4.3.1.67. Can sessions be configured to timeout? If so, what are the configurable

parameters?

Yes. Custom timeout value can be set for session timeouts.

4.3.1.68. Are sessions cleared upon logging off?

Yes.

4.3.1.69. Can active user sessions be forcibly terminated by administrators?

Yes.

4.3.1.70. Describe your approach to managing long-running sessions.

Set alert flag for reviewing such sessions, log entry into suspicious activity log.

4.3.1.71. How does your platform manage user sessions in scenarios where users access

applications from various locations?

We maintain log of each access request including locations from where they are accessed.

4.3.1.72. Explain how your solution assists administrators in remotely terminating active

sessions when necessary.

Admins can see sessions in session dashboard with user details and terminate it after review.

4.3.1.73. Does your solution integrate with Active Roles Server?

No.

4.3.1.74. Explain how your platform complies with industry standards and regulations

related to data security and privacy.

We follow industry standards for data security and privacy by encrypting data during transit, at rest and apply data masking as needed.

4.3.1.75. Vendor must provide three references of clients with similar requirements and user base. Vendor must provide contact information for each reference and current user count range. The estimated range should be greater than 30,000 users.

Badie Designs, Atlanta, Taneka Badie info@badiedesigns.com (>40000 users)

Russell center, Atlanta, Dawn Sizemore, dsizemore@russellcenter.org (>1000 users)

Ayurvedapath, Canada, Dhara Shah, info@ayurvedapath.com (>35000 users)

Our deployment engineers and core team have experience working on SSO IAM implementation for 50000+ users.

State of New Jersey

PHIL MURPHY
Governor

SHEILA OLIVER
Lt. Governor

DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE & ENTERPRISE SERVICES
P.O. BOX 026
TRENTON, NJ 08625-026
PHONE: 609-292-2146 FAX: 609-984-6679

ELIZABETH MAHER MUOIO
State Treasurer

5-YEAR RECERTIFICATION

APPROVED

under the

Minority and Women Business Certification Program

This certificate acknowledges GEOACL LLC DBA:RAINBOW SECURE as a Certified Minority Women Business Enterprise (MWBE) that has met the criteria established by N.J.A.C. 17:46.

This certification will remain in effect for five years.

In order for this certification to remain in effect throughout the 5 year certification period, the business must submit annual verification statements attesting that there has been no change in ownership, control, or any other factor of the business affecting eligibility for certification as a minority or women-owned business. The verification statements must be submitted not more than 60 days prior to the anniversary of the certification approval.

If the business fails to submit the annual verification statement by the anniversary date, or a renewal by its expiration date, the certification will lapse and the business will be removed from the system (SAVI) that lists certified minority and women-owned businesses. If the business seeks to be certified again, it will have to reapply by submitting a new application.

Peter Lowicki
Deputy Director

Issued: 2/3/2023
Certification Number: A0316-34

Expiration: 2/3/2028
The expiration date is contingent on the proper and on-time filing of all Annual Verifications for non-provisional certificates. Please see above for more detail.

Recipient Information

To: BID CLERK DEPARTMENT OF ADMINISTRATION PURCHASING
Company: State of West Virginia Purchasing Division
Fax #: 3045583970

fax

Sender Information

From: Nehal Mehta
Company: GEOACL LLC DBA RAINBOW SECURE
Email address: nehal@rainbowsecure.com (from 24.185.56.104)
Phone #: 7327237955
Sent on: Tuesday, March 26 2024 at 8:43 AM EDT

VENDOR NAME: GEOACL LLC DBA RAINBOW SECURE
VENDOR CONTACT: Nehal Mehta nehal@rainbowsecure.com
BUYER: The State of West Virginia Purchasing Division Larry D McDonnell 304-558-2063 larry.d.mcdonnell@wv.gov

SOLICITATION NO.: CRFP 0947 ERP2400000002
Proc Folder: 1376334
Doc Description: Identity Management Single Sign-On Solution
BID OPENING DATE: 03/26/2024 BID OPENING TIME: 13:30 VENDOR FAX NUMBER: 270-513-9540

Pricing attached here.