CONVERGE
TECHNOLOGY SOLUTIONS

Due Date: April 4, 2024

Response to: State of West Virginia, Department of Administration, Purchasing Division

Request for Proposal: Identity Management Single Sign-On Solution for WV Enterprise Resource Planning Board.

Solicitation No. CRFP 0947 ERP2400000002

Technical Proposal

Submitted By:
Charlie Arnett, Account Executive
Address: 130 Technology Parkway, Peachtree Corners, GA 30092
Phone: 304.549.7698
Email: Charles.Arnett@convergetp.com

Signature: DocuSigned by: Karen Smallwood FD6598FB840A4D2...

CONVERGE
TECHNOLOGY SOLUTIONS

April 4, 2024

Mr. Larry D. McDonnell
State of West Virginia
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Re: WV ERP Board and CRFP ERP2400000002 due 4-4-2024

Dear Mr. McDonnell,

Converge Technology Systems (Converge) is pleased to submit our response for the State of West Virginia's Department of Administration RFP for identity management single sign-on solution.

Converge is looking forward to the opportunity to partner with the State of West Virginia to provide the solution requested in this RFP. As a partner to the State, we offer a mature Identity Access Management (IAM) practice with the experience of customizing solutions to fit your needs. We are committed to exceeding your expectations.

Converge is poised as an extension of your organization, and our objective is to provide you with fair and competitive pricing, and exceptional service. I welcome the opportunity to be of service at any time.

Please note: Features and capabilities described in the technical response are included in the licensing quote and are based upon the implied requirements inferred from the questions provided by the state of WV. If any features/capabilities are deemed unnecessary in initial or future phases of the implementation, the quote can be adjusted accordingly.

Please do not hesitate to contact me if you require additional information or have any questions. On behalf of Converge, I would like to thank you for the opportunity to participate in this process.

Sincerely,

Charlie Arnett
Senior Client Executive
304.549.7698

Table of Contents

4.1. Background and Current Operating Environment:

Currently the State of WV uses MyApps custom identity management system. This system was developed by the Auditor's office in 2008. This system was also used to manage user access when the WVOASIS system went live in 2013 for Budget, 2014 for Financials and starting in 2015 for the HRM, time and leave system.

There is now a need to standardize on a new platform that will allow the State to manage login profiles with greater efficiency and with greater security standards. The Enterprise Resource Planning Board is issuing this RFP to find a cloud based comprehensive single sign on solution for the use of many third-party applications to include CGI Advantage, UKG, Deighton, and other applications currently hosted and maintained by the ERP Board.

4.2. Project Goals and Mandatory Requirements:

In the past three years the OASIS system has been requested to provide multiple forms of data to the critical agency system to include some of those listed above. This helps in the reduction of duplication of data, duplication of user entry of this data and to provide a central source for data. As this expands in the future, there needs to be a secure mechanism for user interaction. That user interaction we believe will come from a new cloud-based identity management system. Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches.

4.2.1. Goals and Objectives

4.2.1.1 Provide a state-wide solution for the ERP solution and supporting applications to provide a single sign on solution.

Okta is the complete state-wide identity solution for all your apps and people that's universal, reliable, and easy. Okta's comprehensive, complementary, and flexible identity cloud solves every identity use case, regardless of the audience or user. Okta pioneered cloud-based identity, offering enterprise-grade reliability and world-class security while prioritizing customer success for customers of all sizes.

2009	18,000+	7,000+	19	7 years
Founded	Customers	Employees	Global Offices	Magic Quadrant Leader

Okta's fully managed software-as-a-service solution is delivered as a multi-tenant service built from the ground up. Customers benefit from regular product updates, 99.99% availability with zero planned downtime, pre-built UIs, and comprehensive documentation that streamlines time-to-value for our customers. These are some of the reasons why Okta continues to be the leader in both Gartner's Access Management Magic Quadrant and Forrester's Identity as a Service Wave as well as Gartner's Customers' Choice in Access Management.

4.2.1.2 Obtain a complete single sign solution that is cloud based and will provide robust security solutions to include encryption, logging, and provide common industry standard options for a single sign on solution.

The Okta Identity Cloud is a complete secure, complete single sign on solution for the State of West Virginia. The Okta Identity Cloud easily integrates into existing application landscapes by providing a transparent, vendor-neutral identity platform that supports industry standard protocols such as SAML, SCIM, OAUTH2 and WS-Fed. With the Okta Integration Network (OIN), we offer a catalog of 7,500+ pre-built application integrations, including many of the most common enterprise applications, end-user directories, and identity solutions, such as Workday, Office 365, Salesforce, and ServiceNow. Each application in the OIN comes complete with step-by-step, guided configuration instructions that greatly reduce the time required for integration with Okta. For a fully indexed list of our out-of-the-box applications, please see https://www.okta.com/integrations/

On-premises, Okta offers direct integrations into AD & LDAP through our AD/LDAP Agents and offers flexibility in connecting to other custom on-prem user stores. Okta leverages these integrations to provide a single point of control for authentication and can centralize and link these disparate user stores centrally through Okta's Universal Directory.

Okta's compliance program is built upon industry-standard certifications and authorizations, including SOC 2 Type II, ISO 27001:2013, ISO 27017;2015, ISO 27018:2019, Cloud Security Alliance STAR Attestation /

Level 2. Okta is FedRAMP Moderate and FedRAMP High authorized, complying with more than 420 baseline security controls for handling mission-critical information, as well as DOD IL4 authorized with a Provisional Authorization to service IL5 environments.

Okta logs industry-standard events as defined by US FedRAMP & NIST standards, including, but not limited to: successful / failed logins, successful / failed connection attempts, privileged user access and activities, processes, object accesses. Log entries include applicable information such as date/time, event type, message, outcome or actions, userID or account, source / destination IP, port, protocol, and other relevant information.

Okta is the right choice for the largest organizations looking to rationalize their IT spend and consolidate their Identity and Access Management (IAM) systems. All our strengths in IAM are reinforced by our organizational structure (number of engineers focused on identity) and investments (R&D spend, venture funding, and acquisitions) driving Okta's leadership in the industry.

Value for the State of West Virginia

- Cloud-first architecture leads to increased operational efficiency (lower TCO)
- Built-in high availability, scalability, and security with 99.99% uptime for every customer. Avoid building out and supporting your own infrastructure (load balancers, HA, etc.).
- One single service to meet all your Universal Identity Profile Management requirements; no need to install & manage multiple servers across cloud, on-prem, and directory services.
- Manage all users and applications from one interface. No requirement for users to be managed in different directories, DBs, apps, etc.
- Broadest and deepest application network for single-sign-on and user lifecycle management
- Real-time policy-driven automated provisioning capabilities.
- Rapid development through pre-built, customizable widgets and SDKs with detailed supporting documentation.
- Comprehensive APIs (registration/extensible profile management, authentication, multi-factor authentication (MFA), lifecycle management, policies & entitlements).

4.2.2 Mandatory Project Requirements

The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

4.2.2.1 The solution must be able integrate with our existing identity sources including Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Ultimate Kronos Group (UKG)

Compliant. Okta's Universal Directory is a robust cloud-based directory service that enables organizations to integrate with multiple identity stores simultaneously, including Active Directory, V3-compliant LDAP directories, and third-party human resources management systems (HRMS) solutions (e.g., Workday, PeopleSoft, UKG, etc.). Universal Directory acts as a meta-directory that synchronizes information across disparate user stores as attributes. Okta can combine both Okta-sourced users AND users sourced by an external directory (i.e., LDAP) within Universal Directory. Universal Directory can also be used independently, without any external directory.

4.2.2.2 The solution must provide a seamless migration path for users from our existing identity infrastructure.

Okta provides customers multiple ways to seamlessly migrate their user profiles from an existing user repository into Okta, including the three primary categories:

- Bulk import
- Just-in-time
- Existing directories

Bulk Import

With a bulk import, you pre-load (also known as pre-staging) all the user profiles into Okta before the go-live date of your migration. This method is a back-end process that creates all the users at once before they start using the Okta system rather than one at a time, as is done with the just-in-time method. Since the entire import occurs ahead of time, the bulk method can help reduce many issues that users might typically encounter with other types of migrations. It also gives the import time to process the various tasks involved in properly setting up each user profile. You can perform a bulk import by doing either a CSV import or by using one of the two Okta Users API methods.

A CSV import gives you the flexibility to import a user base from any system that has the ability to export the user base into a CSV format. In spite of that flexibility, CSV imports are not designed for large scale

migrations. Additionally, passwords cannot be imported using this method and will require users to set their passwords when they first log in to the system. To perform a CSV import you use an Okta provided CSV file to serve as a base template for your users. From the People page of the Okta administration user interface you can import the template file directly into the Okta Universal Directory once you've added all the users to the template.

Just-In-Time

Just-In-Time is a method of creating users on demand as they log in to Okta for the first time. You can perform a Just-In-Time migration using the inbound federation method or one of two existing database methods.

Just-in-time methods can simplify your migration since they automate the process and only create new users if they don't already exist in Okta. While in some ways just-in-time methods are easier than importing users in bulk, they can cause users to experience delayed login times if there's a large influx of new user logins once Okta goes live. However, there are ways you can prevent this through rate limit adjustments and performance testing.

For an inbound federation just-in-time migration you can use an existing trusted authentication provider to sign into Okta. This is also known as a federated login. You can do this using any SAML 2.0 supported application or social authentication provider, such as Facebook, Google, LinkedIn, and Microsoft. That also includes any OIDC/Oauth 2.0 compliant provider. When using inbound federation, you can enable just-in-time to automatically create a new user account in Okta if the federated account logging in does not already exist in Okta. This automates and speeds up user creation since it can pull the user identity information directly from the identity provider. The user password will not be set in Okta at this point, but their identity attributes will be imported.

Existing directory migrations

You can also migrate user profiles using an existing directory, such as Active Directory, LDAP, a CRM cloud app, or other on-premises user repositories. Typically, these migrations leverage a small agent running on the directory or use one of the 130+ pre-existing provisioning integrations provided in the Okta Integration Network to automatically import the users from your existing directory system.

You can choose from the following methods for existing directories:

- Directory imports (Active Directory/LDAP)
- App import (CRM)
- On-premises provisioning

4.2.2.3 Authentication methods must include SAML2.0, SP (Service Provider) and IDP (Identity Provider) methods of authentication.

Okta fully supports SAML 2.0 as well as SP and IDP methods of authentication.

4.2.2.4 The solution presented must be cloud-based.

Okta is a cloud-based Identity as a Service (IDaaS) solution born and built in the cloud. The Okta Identity Cloud is a true Software as a Service (SaaS) offering that is multi-tenant (i.e. Okta is not just a hosted VM solution).

While Okta is cloud-based, it includes several integration components that enable hybrid-cloud environments to leverage Okta. This includes the following on-premise components:

- **Okta Active Directory Agent:** A lightweight agent that can be installed on any Windows Server and is used to connect to on-premises Active Directory for user provisioning, de-provisioning, and authentication requests.
- **Okta LDAP Agent:** A lightweight agent that can be installed on any Windows or Linux Server and is used to connect to on-premises V3 compliant LDAP directories for user provisioning, de-provisioning, and authentication requests.
- **Okta Radius Agent:** A light weight agent that provides RADIUS services to RADIUS clients (e.g. VPNs, Linux/Unix environments, etc.) so that Okta authentication and multi-factor authentication services can be leveraged.
- **Okta Provisioning Agent:** A lightweight agent that enables SCIM 2.0 based provisioning to on-premise applications via the Okta Identity Cloud. The Okta Provisioning Agent can also be integrated with the Okta SCIM Server to enable on premise provisioning to applications that don't support SCIM (e.g. databases, API-based application, etc.).

4.3. Qualifications and Experience:

Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

Qualification and Experience Information: Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

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. Okta has numerous REST-based APIs to allow flexibility in developing a solution that best fits your needs. Okta offers the following APIs:

Authentication API – Supported SDKs Include:

- ANDROID
- ANGULAR
- REACT
- IOS
- GO
- JAVASCRIPT
- VUE.JS
- JAVA
- .NET
- NODE.JS
- PHP
- PYTHON

Management APIs

- Authorization Servers
- Apps
- Events
- Dynamic Client Registration
- Factors
- Groups
- Identity Providers

- Linked Objects
- Policy
- Administrator Roles
- Schemas
- System Log
- Templates
- Trusted Origins
- Users
- Zones

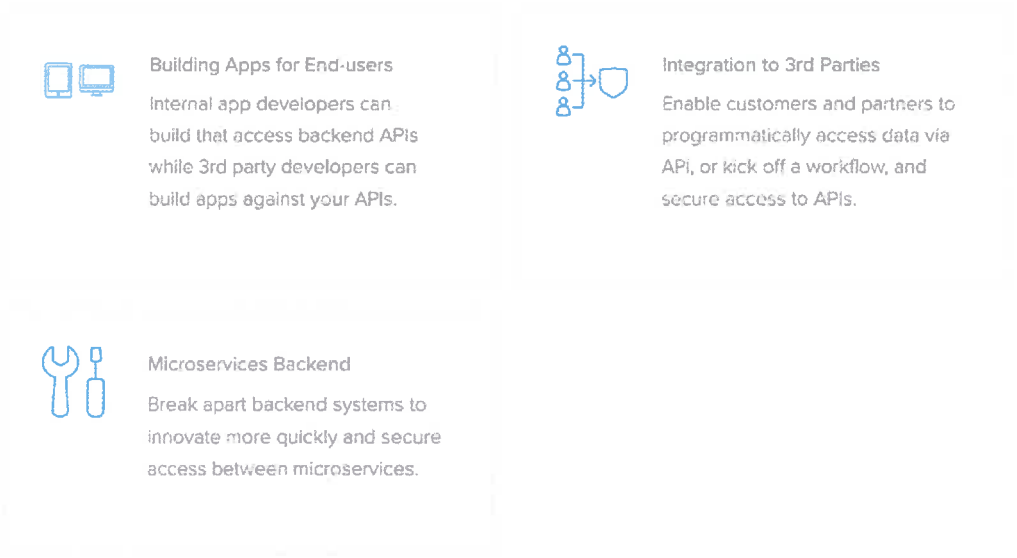
Please refer to the following link for more information regarding Okta's APIs: https://developer.okta.com/

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.

Okta's API Access Management is a cloud-based OAuth 2.0 authorization server specifically designed for securing API endpoints. API Access Management can be leveraged to create fine-grained scopes and claims to be used within the OAuth 2.0 specification. Okta centralizes and manages all user and resource access to an API via authorization servers and OAuth access tokens, which an API gateway/API Management solution can then use to make allow/deny decisions. This setup allows for fine-grained, centrally-managed control, so organizations can easily provision and deprovision access to APIs.

Okta API Access Management provides identity-driven authorization for any app or service, with user-friendly and centralized administration across all of an organization's APIs. Features include:

- **OAuth 2.0 API Authorization**
  - Complete standard-compliant support for OAuth 2.0
  - Proven compatibility with 3rd party API management solutions
  - Designed for modern web and mobile applications, and service-to-service scenarios
- **Flexible Identity-Driven Policy Engine for Any Type of User or Service**
  - Flexible policies that define access based on user profile, groups, network, client, and consent
  - Instant access revocation or updates to user permissions based on user profile and status



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.

Yes, Okta provides API token management and creation. See 4.3.1.2

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

Okta has numerous REST-based APIs to allow flexibility in developing a solution that best fits your needs. Okta offers the following APIs:

Authentication API – Supported SDKs Include:

- **ANDROID**
- **ANGULAR**
- **REACT**
- **IOS**
- **GO**
- **JAVASCRIPT**
- **VUE.JS**
- **JAVA**
- **.NET**
- **NODE.JS**
- **PHP**
- **PYTHON**

Management APIs

- **Authorization Servers**
- **Apps**
- **Events**
- **Dynamic Client Registration**
- **Factors**
- **Groups**
- **Identity Providers**
- **Linked Objects**
- **Policy**
- **Administrator Roles**
- **Schemas**
- **System Log**
- **Templates**
- **Trusted Origins**
- **Users**
- **Zones**

Please refer to the following link for more information regarding Okta's APIs: https://developer.okta.com/

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

Okta's API Access Management is built on Okta's Universal Directory which allows Sign On and Authorization Policies that limit particular OAuth 2.0 scopes to specific devices, a specific network, and even group membership. Further, specific scopes can require user consent to ensure the user explicitly authorized access for the application. Most importantly, a security team can manage those policies outside the API gateway while centrally logging access requests, grants, and policy changes. For additional compliance needs, access information can also be viewed via the Okta UI or exported to a 3rd party system (such as SIEM/ticketing systems). By shifting the IT department from blockers to enabling developers with simple integrations using well-established standards and tools, it shifts APIs out of the realm of "shadow IT" and back to trusted, known systems.

All communication between Okta and the customer is protected by TLS 1.2 capable services supporting Perfect Forward Secrecy (PFS) and AES 256-bit encryption. Okta also utilizes HTTP Strict Transport Security (HSTS) which prevents the down-grade of HTTPS communication to clear-text HTTP.

Stored data is encrypted using AES and a 256-bit encryption key specifically created for the customer (with each customer assigned their own).

Amazon Web Services (AWS) provides the infrastructure that hosts Okta's identity-as-a-service platform (IDaaS). Customer-specific cryptographic keys are protected using the AWS KMS service and a FIPS 140-2 Level 2 certified hardware security module with Level 3 physical protection.

See AWS KMS Cryptographic Details: https://docs.aws.amazon.com/kms/latest/cryptographic-details/intro.html

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

Yes. Okta supports the following protocol/standards and more:

- **Federation Identity Standards:** SAML (1.1 and 2.0), WS-Fed, and OpenID Connect.
- **Delegated Authorization:** OAuth 2.0
- **User Provisioning:** SCIM 1.1 and 2.0
- **Authentication / MFA Standards**: AD, LDAP, WCP, RADIUS, FIDO U2F, FIDO2 WebAuthN, HTTP Headers, Kerberos, TOTP

4.3.1.7. Detail the scalability of your Application Programming Interface infrastructure to support high volumes of authentication and authorization requests.

The Okta service is built on an on-demand cloud architecture. Our highly differentiated cell architecture is a self-contained instance of the entire Okta service. Each cell has its own set of Job/Database servers, Load Balancers and App Servers and is capable of hosting user identities independent of other cells. Okta spins up additional cells as needed, with each having its own complete high availability, high performance architecture to help scale the system and host additional users if the need arises. Okta's service and operations are specifically designed to scale against demand for users (on-boarding new identities) and concurrent usage (# of user Authentications) which allows Okta to onboard large customers in a predictable and scalable fashion.

Please refer to the following whitepapers for more information:

Not all Cloud Services are Built Alike: https://www.okta.com/resources/whitepaper/how-okta-builds-and-runs-scalable-infrastructure/

Scaling Okta to 50 Billion Users: https://www.okta.com/resources/whitepaper/scaling-okta-to-billions-of-users/

4.3.1.8. Does your solution provide Remote Authentication Dial-In User Service (RADIUS) support that does not require on-premise components?

Yes. Okta has a RADIUS agent which allows Okta to authenticate users accessing resources that utilize RADIUS. For example, firewalls or network services like Wi-Fi will be configured to use RADIUS authentication. Okta can then apply MFA policies for authentication.

Okta also can be configured to allow Integrated Windows Authentication, where users who log into a Windows domain are automatically authenticated to Okta, and provided Single Sign-on into cloud applications seamlessly.

For more information, please see:

https://help.okta.com/en-us/content/topics/integrations/getting-started.htm

https://help.okta.com/en-us/content/topics/integrations/radius-best-pract.htm

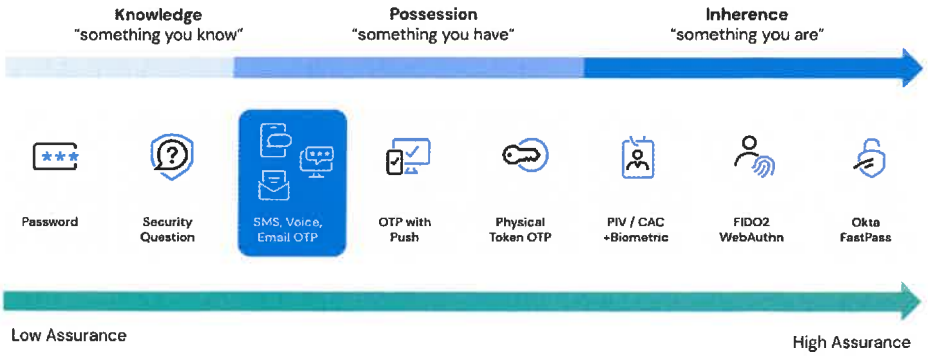
4.3.1.9. Indicate if the solution provides supported push notification. If so, what controls can be used to lower the risk of push fatigue attacks.

Yes. Okta supports push notifications. Okta enables customers to combine "number challenges" with the Okta Verify app to prevent against "MFA Fatigue" attacks.

4.3.1.10. List the Multi-factor methods supported.

Okta's MFA provides both the highest security and simplest administration possible. Okta's native multi-factor options can be centrally administered in an integrated fashion. Any factor supported in Okta can be used for passwordless authentication.
Okta built-in authenticators:

- **Okta Verify OTP (soft token) on iOS, Android**
- **Okta Verify w/ Push (soft token, with app registration / certificate) on iOS, Android**
- **Okta FastPass (MacOS, Windows, iOS, Android)**
- **SMS**
- **Voice**
- **WebAuthn (Biometric authentication, including Touch ID and Windows Hello)**
- **Yubikey**
- **Smartcard / certificate-based authentication is supported for workstations that authenticate to Windows domain via these methods, and Okta via Windows Credential Provider (WCP)**



3rd Party MFA products integrated to Okta and interoperable:

- **Duo Security**
- **RSA SecureID**
- **Symantec VIP**
- **Any 3rd party solution supporting OATH including Gemalto and Safenet**
- **Custom SAML/OIDC authenticators**
- **Google Authenticator**

Okta uses IP reputation data, User behavior context, device trust, and risk level checks, which can be layered on top of the passwordless authentication for an additional layer of security.

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

Yes. The following brute-force/password-guessing mitigation is embedded in or provided by Okta:

- Rate-limiting and throttling on authentication requests
- Configurable account lock-out
- Basic MFA included
- Advanced MFA policy features available as add-on
- Configurable IP Zone restrictions
- Detailed event logs available through UI and API
- API access that can be leveraged by customers to implement additional measures as needed

In addition, the platform undergoes routine external penetration tests and internal security assessments by offensive security engineers. These tests include a comprehensive range of types of authentication abuse to catch flaws that may have been introduced before they can have any negative impact on customers.

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.

Okta leverages an internal team of engineers who continuously monitor, detect, and respond to security pertinent events generated by our systems. We will implement global blocks if brute-force attempts are affecting a large number of customers, or if they're causing availability or stability issues with the Okta platform.

Because we cannot risk causing false-positives, we need to be very accurate in what we block. Customers who are comfortable with the possibility of false-positives can block wider ranges and potentially gain more protection.

The following brute-force/password-guessing mitigation is embedded in or provided by Okta:

- Rate-limiting and throttling on authentication requests
- Configurable account lock-out
- Basic MFA included
- Advanced MFA policy features available as add-on
- Configurable IP Zone restrictions
- Detailed event logs available through UI and API
- API access that can be leveraged by customers to implement additional measures as needed

In addition, the platform undergoes routine external penetration tests and internal security assessments by offensive security engineers. These tests include a comprehensive range of types of authentication abuse to catch flaws that may have been introduced before they can have any negative impact on customers.

All communication between Okta and the customer is protected by TLS 1.2 capable services supporting Perfect Forward Secrecy (PFS) which creates a unique TLS session key meaning an attacker with Okta's private keys could not read previously captured traffic via sniffing or man-in-the-middle attacks. We also utilize HTTP Strict Transport Security (HSTS) which prevents the down-grade of HTTPS communication to clear-text HTTP.

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.

Okta built-in authenticators include:

- Okta Verify OTP (soft token) on iOS, Android
- Okta Verify w/ Push (soft token, with app registration / certificate) on iOS, Android
- Okta FastPass (MacOS, Windows, iOS, Android)

- SMS
- Voice
- WebAuthn (Biometric authentication, including Touch ID and Windows Hello)
- Yubikey
- Smartcard / certificate based authentication is supported for workstations that authenticate to Windows domain via these methods, and Okta via Windows Credential Provider (WCP)

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

Okta's Adaptive Multi-factor Authentication is an additional layer of security designed to consider user behavioral patterns and context when evaluating login attempts. Okta's Adaptive Multi-factor Authentication leverages a number of contexts, including:

- Device Context
- Location Context
- Network
- Application Context
- User and Group

Each context represents a family of signals such as IP address, Country, Device ID, etc. to understand a user's typical login patterns. Admins can build smart adaptive authentication policies and request for MFA step-up authentication only when a user deviates from normal login patterns.

Okta's Adaptive MFA also includes capabilities around Okta's Risk Engine, which is designed to ingest third party signals to inform access decisions and to aid in continuous authentication. In addition to user, location, device, and network context, Okta can take in the following signals from third parties:

- Mobile Device Management (MDM): Okta can utilize and integrate with any MDM on the market (VMware Airwatch, Intune etc) to help inform access decisions based upon user device context, and whether that device is managed or not.
- Endpoint Detection and Management: Okta can integrate and ingest signals to inform Risk scoring from Windows Defender and Crowdstrike products
- Email Security: Okta can integrate with best-of-breed email security providers such as Barracuda, Office365, Google, Proofpoint, Mulesoft, etc.

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

Yes. Okta supports inbound federation (Okta as a Service Provider) from third-party identity providers such as SAML 2.0 providers, or Social Authentication (Facebook, Google, Microsoft, LinkedIn), which can be leveraged to generate authentication to downstream applications using the standards that are supported above. This includes both end users and administrators of the Okta Identity Cloud service.

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.

Okta supports the following protocol/standards and more:

- Federation Identity Standards: SAML (1.1 and 2.0), WS-Fed, and OpenID Connect.
- Delegated Authorization: OAuth 2.0
- User Provisioning: SCIM 1.1 and 2.0
- Authentication / MFA Standards: AD, LDAP, WCP, RADIUS, FIDO U2F, FIDO2 WebAuthN, HTTP Headers, Kerberos, TOTP
- Form fill credential vault using Okta's Secure Web Authentication (SWA)
- Authorization Policy Engine: OPA
- Privileged Access: SSH, RDP
- Transport Security: HTTPS, TLS

4.3.1.17. Explain how your solution adapts authentication methods based on contextual factors like location and device.

Okta's Adaptive Multi-factor Authentication is an additional layer of security designed to consider user behavioral patterns and context when evaluating login attempts. Okta's Adaptive Multi-factor Authentication leverages a number of contexts, including:

- Device Context
- Location Context
- Network
- Application Context
- User and Group

Each context represents a family of signals such as IP address, Country, Device ID, etc. to understand a user's typical login patterns. Admins can build smart adaptive authentication policies and request for MFA step-up authentication only when a user deviates from normal login patterns.

Okta's Adaptive MFA also includes capabilities around Okta's Risk Engine, which is designed to ingest third party signals to inform access decisions and to aid in continuous authentication. In addition to user, location, device, and network context, Okta can take in the following signals from third parties:

- Mobile Device Management (MDM): Okta can utilize and integrate with any MDM on the market (VMware AirWatch, Intune etc) to help inform access decisions based upon user device context, and whether that device is managed or not.
- Endpoint Detection and Management: Okta can integrate and ingest signals to inform Risk scoring from Windows Defender and CrowdStrike products
- Email Security: Okta can integrate with best-of-breed email security providers such as Barracuda, Office365, Google, Proofpoint, MuleSoft, etc.

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

If a user has lost their device used for MFA (i.e. used for Okta Verify, Google Authenticator, etc.) that user can use another configured factor for MFA like an email address or security question to log in to their Okta Dashboard. Once into the Okta Dashboard, Okta provides the user with self-service options for resetting any of their configured MFA factors, in this case, setting up a new device to be used with MFA.

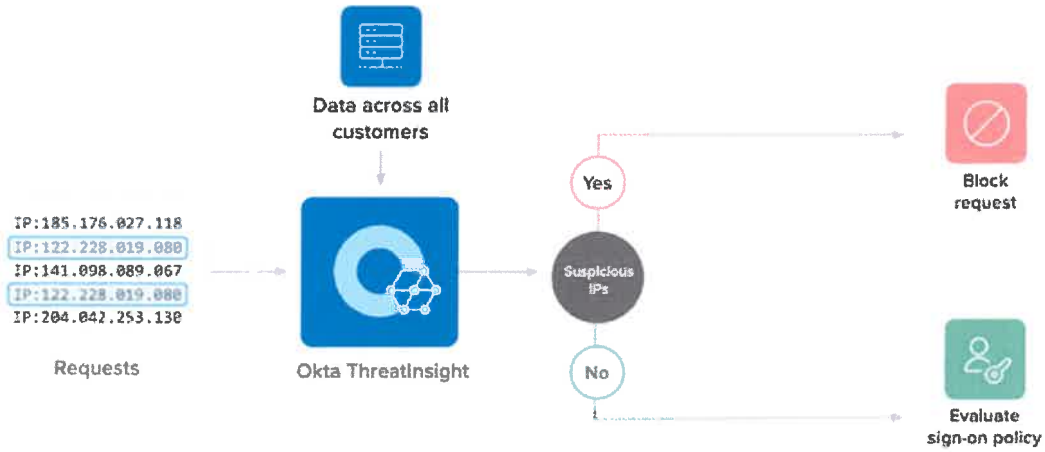
If the user did not configure additional authenticators other than the lost device, an Okta administrator can reset one or more authenticators connected to that device for the user. At next login, the user will be prompted to set up these factors on their new, replacement device.

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

Geo-location/fencing is supported as a part of Adaptive Multi-factor Authentication and is fully configurable by administrators through the Administrator UI.

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

Okta also offers service level threat protection to every Okta customer via Okta ThreatInsight, which uses heuristics (static rules) and machine learning to observe and derive intelligence from credential-based attacks detected across Okta's customer base. ThreatInsight captures IP addresses accessing Okta across all customers and checks for IPs that are causing password spray and brute force attacks. These IPs are marked as suspicious and put into the ThreatInsight pool, giving admins the option to block or audit access from those IP addresses in their own org. ThreatInsight is evaluated pre-authentication to prevent user lockout.



The detection of a threat takes place prior to authentication evaluation. Requests that are blocked by Okta ThreatInsight prevent user lockouts from suspicious IP addresses. Admins can configure Okta ThreatInsight to detect suspicious IP addresses from credential-based attacks. When Okta ThreatInsight actions are enabled, end users may sign in to their org as usual. If a sign-in attempt from a malicious IP address is detected and authentication requests are set to be blocked, the user receives an HTTP 403 error.

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

Yes. Okta's Adaptive Multi-Factor Authentication leverages a number of contexts, including:

- Device Context
- Location Context (e.g., impossible travel)
- Network
- Application Context
- User and Group

Each context represents a family of signals such as IP address, Country, Device ID, etc. to understand a user's typical login patterns. Admins can build smart adaptive authentication policies and request for MFA step-up authentication only when a user deviates from normal login patterns.

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

Okta detects and prevents unauthorized access through a combination of adaptive multi-factor authentication (AMFA), security policies based on user behavior and context, and integration with network security tools. Adaptive MFA dynamically adjusts authentication requirements based on risk factors, such as login location or device. Security policies can restrict access to sensitive resources based on user roles, geolocation, and device state. Okta also offers insights and reporting tools for monitoring and responding to suspicious activities, enhancing the organization's overall security posture.

Okta integrates with network security tools, including endpoint detection and response (EDR) solutions, to enhance security and streamline access decisions. The integration works by leveraging Okta Verify together with EDR solutions to probe devices for context and trust signals when users attempt to access protected resources. These signals are evaluated against configured authentication policies in the Okta Admin Console, which then determines the access decision. Okta currently supports integrations with several major EDRs, such as CrowdStrike and Microsoft Windows Security Center.

For details, please refer to https://help.okta.com/oie/en-us/content/topics/identity-engine/devices/edr-integration-main.htm

Read more about the risk adaptive capability in sections 4.3.1.64 and 4.3.1.65.

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

Yes, both Attribute-based Access Control (ABAC) and Role-based Access Control (RBAC) can be achieved by defining Okta Groups with roles. Rules can then be created that auto populate users to certain Role Groups, which then automatically provisions them to applications assigned to that role. Groups are commonly used to assign SSO access within Okta and to provision users to apps with specific entitlements (roles, profiles, etc). When rules are configured to populate groups based on attributes, you achieve ABAC and RBAC.

Okta can also empower ABAC and RBAC within the downstream applications it is authenticating access to. Okta allows admins to customize the attributes passed back to the applications in the SAML assertions or OIDC ID Tokens. These custom attributes can then be utilized by the application in question to customize the experience of the user based on attributes contained in the user's profile within Okta.

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

Okta can support identity brokering natively. Okta can act as an identity broker for the applications/Service Providers that are integrated with Okta. Okta has the ability to integrate with any Open ID Connect or SAML 2.0 IDP, as well as social connections, to allow those IDPs to perform authentication to the SP. Users can be presented with options on how they would authenticate to the SP, either via buttons embedded on Okta's Sign In Widget that directs the user to the correct IDP to authenticate. The other way is for admins to define with Okta calls "routing rules", which direct end users to identity providers based on the user's location, device, email domain, attributes, or the app they are attempting to access. Examples of these routing rules include members of @domainx.com being routed to an IDP to authenticate to an app, which members of @domainy.com being routed to IDP B for authentication to the same app.

More information about Okta's 3rd party IDP support can be found here: https://help.okta.com/en-us/Content/Topics/Security/Identity_Providers.htm

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. Okta's Adaptive Multi-Factor Authentication leverages a number of contexts, including:

- Device Context
- Location Context (e.g., impossible travel)
- Network
- Application Context
- User and Group

Each context represents a family of signals such as IP address, Country, Device ID, etc. to understand a user's typical login patterns. Admins can build smart adaptive authentication policies and request for MFA step-up authentication only when a user deviates from normal login patterns.

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

Okta enforces the principle of least privilege access by ensuring that users only have the minimum level of access required for their roles or functions. The implementation of least privilege access within Okta involves auditing existing accounts and credentials to ensure appropriate permissions, employing privilege bracketing to limit access rights, and utilizing single-use credentials with expiration policies to restrict access to sensitive data and information.

Just-in-time granular access can also be granted using time-limited privileges or one-time-use credentials to temporarily allow a higher level of authorization to specific users who need it to complete a certain task. Once this is complete, the credentials are removed to avoid privilege creep.

More details available at https://www.okta.com/identity-101/minimum-access-policy/

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

Okta Session Timeouts can be configured by customer Okta administrators. Options include:

- Maximum Idle Session Time
  - This property is configurable from the Okta Admin console: https://help.okta.com/en/prod/Content/Topics/Security/healthinsight/session-lifetime.htm
  - Maximum number of minutes that a user session can be idle before the session is ended.
  - Idle sessions consist of the user not interacting with Okta org domain specific links (App/Chiclet links, Okta Admin console, etc).

- Maximum Session Time
  - This property is only able to be configured using Okta Policy API endpoints: https://developer.okta.com/docs/reference/api/policy/
  - Maximum number of minutes from user login that a user session will be active.
  - The time set here will force the user to sign-in after the specified number of minutes.

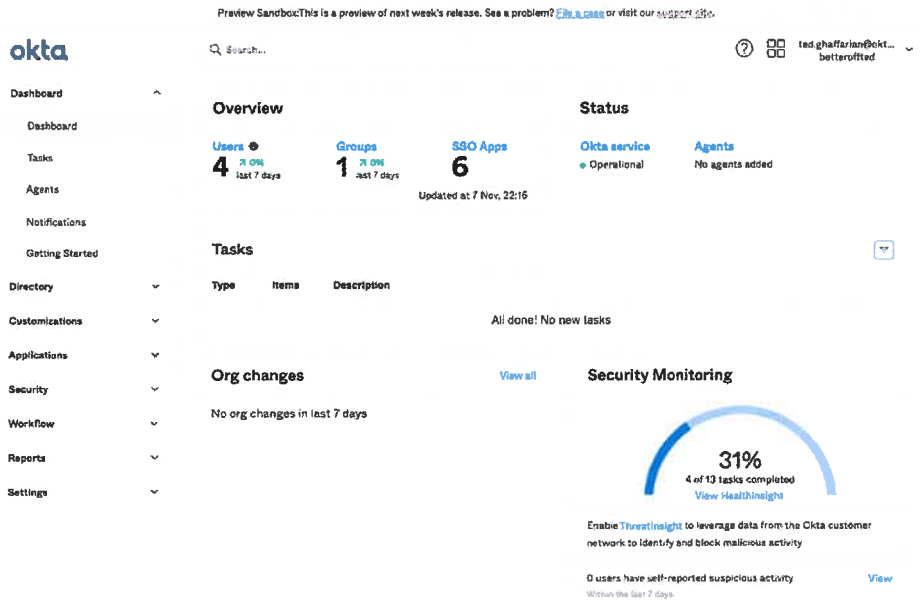
App Session timeouts: Okta session timeouts have no impact on applications configured in an Okta org but Okta Workflows has an event (User Signed Out: https://help.okta.com/en/prod/Content/Topics/Workflows/connector-reference/okta/events/usersignedout.htm) that could be used to terminate sessions in downstream. This is dependent on the downstream app's capability to terminate sessions programmatically.

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

Okta offers a sandbox environment, where your dev team can test implementations, integrations, and other functions before deploying into their production environment. Utilizing a sandbox environment within your infrastructure provides multiple benefits for IT departments to ensure their systems are properly integrated and tested.

Full Testing Environment

Okta's true multi-tenant architecture enables the creation of a full-feature sandbox environment for your company. This means you have complete access to a second fully functioning version of Okta to test things like AD integrations and application configurations prior to pushing them out to your full set of users. If you are trying out new features or adding new integration points to Okta, you can also test these within the sandbox environment.



Pre-Release Features

The Okta Preview Sandbox is unique in that it also provides access to new features one week prior to production release; these preview features are not exposed to your end users. This means you have one week to familiarize yourself with new features prior to full release.

Automatic Updates

As with Okta's full-production environment, the Preview Sandbox is updated automatically each week, so you never have to worry about scheduling and installing new features. In addition, new features that are made available in Preview Sandbox are automatically introduced to the production version without any work required by your IT department.

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

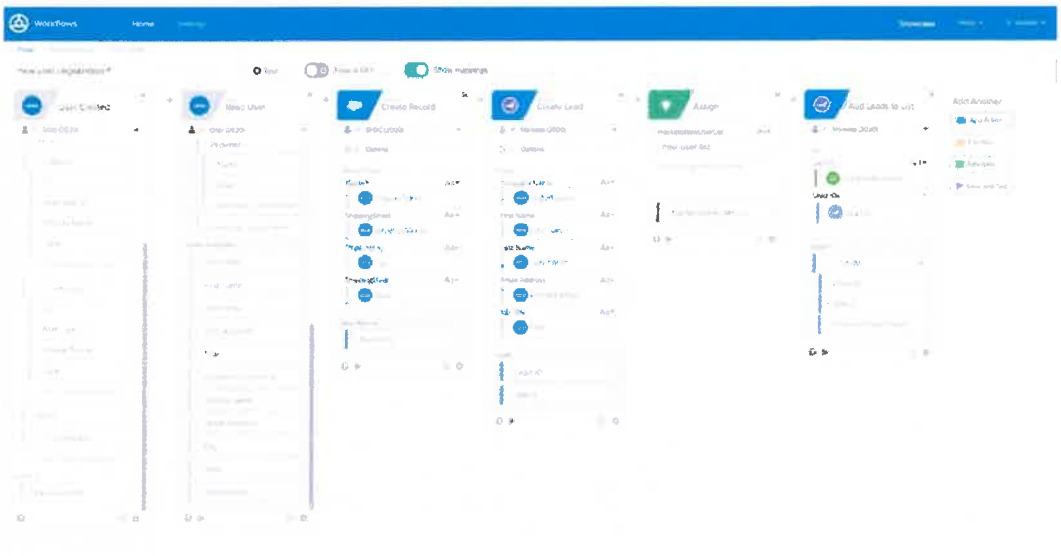
Yes. Okta offers a sandbox environment, where your dev team can test implementations, integrations, and other functions before deploying into their production environment. Utilizing a sandbox environment within your infrastructure provides multiple benefits for IT departments to ensure their systems are properly integrated and tested. See the response to the previous question (4.3.1.28) for more information.

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

Yes. Okta has numerous REST-based APIs to allow flexibility in developing a solution that best fits your needs. Okta Workflows is also available to automate tasks without the need for complicated scripts. Furthermore, you can use the Okta Expression Language throughout the Okta Admin Console and API for the Okta Identity Engine. The Okta Expression Language is based on SpEL (https://docs.spring.io/spring-framework/docs/3.0.x/reference/expressions.html). Expressions allow you to reference, transform, and combine attributes before storing them on a user profile or passing them to an app for authentication or provisioning. For example, you might use a custom expression to create a username by stripping @company.com from an email address. Or, you might combine the FirstName and LastName attributes into a single DisplayName attribute.

Okta Workflows is a no-code automation and orchestration platform that enables admins to modernize ever-more-sophisticated identity-centric processes without leaning on developers. Workflows can be used to augment Lifecycle Management and provide custom logic for organization-specific use cases. It provides a graphical drag-and-drop interface that combines triggers, logic, and time-based actions to build powerful "if-this-then-that" flows. As a result, anyone can easily stitch together app-specific provisioning and deprovisioning tasks.

For instance, with Okta Workflows, you can leverage Okta's library of pre-built connectors for apps like Box, Slack, Salesforce, and more (or connect via public APIs) to tailor processes with deeper actions that meet your precise requirements. With out-of-the-box functions for flow control, branching, and data manipulation, Okta offers the power of code without code, and it is finally possible to orchestrate identity tasks that were previously just too hard to automate. By having this capability built-in to your identity architecture, your team will increase agility and decrease costs, all while facilitating constant business change and improving your company's security posture.



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. Unlike other identity management solutions, Okta is not simply a toolkit that you use to connect your web applications to your user directories. That takes too much of your time and resources. Instead, Okta "integrates" applications into its service for you, and you simply deploy these pre-integrated applications to your users as necessary. You can authenticate these users against your own user store (e.g. Active Directory or LDAP) or you can use Okta as the user store. Okta is unique in providing quick, feature rich integrations with web based and native mobile applications, whether these are in the cloud, on-premises or on your smartphone or tablet. These integrations are delivered as a part of the Okta service and include both SSO and user management capabilities.

For typical cloud-based applications (e.g., Salesforce, Google Apps, Workday, etc.), these integrations are delivered as a part of Okta's Integration Network (OIN), which has over 7,500 pre-built integrations. Administrators simply select from Okta's list of thousands of supported applications, use a simple wizard answering basic questions about their specific instance of the applications (such as URL and administrative IDs) and Okta handles the rest. All technical details (such as SSO protocols and user management API implementations) are encapsulated in the service and continually maintained by Okta on your behalf. These applications may use a standard like SAML or OpenID, they may use a proprietary API, or they may use Okta's Secure Web Authentication (SWA) protocol.

Many of the most popular on premises web-based applications (Oracle Apps, Lawson, Jira, etc.) are also included in the Okta Integration Network. For custom developed on-premises web based applications Okta provides a range of integration options as well. Secure Web Authentication integration for SSO can be

easily added, Okta has SAML toolkits that can be used to SAML enable your apps, and Okta also supports provisioning and deprovisioning into applications that expose user management APIs publicly.

Okta also provides easy access to mobile enterprise applications from any device. Whether your enterprise apps are HTML5 web apps optimized for mobile platforms or native iOS or Android apps, Okta has a solution. Any web application in the Okta Integration Network can be accessed with single sign on from any mobile device. Mobile web apps can use industry standard SAML, or they can use Okta's Secure Web Authentication SSO technology. Native applications like Box Mobile can be integrated using SAML authentication for registration and OAuth for ongoing use.

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

Yes. Okta is a highly user-friendly system, with much of the configuration and management done through easy to follow wizards. This greatly decreases the need for heavy documentation for deploying and administering Okta.

Documentation

The Okta Identity Cloud offers tremendous developer resources including robust documentation (API reference and quick start), a thriving developer community, blogs, pre-built widgets, SDK, example code across multiple programming languages, and a wide range of examples on GitHub. In addition to providing a comprehensive RESTful API, Okta offers several Server SDKs and Client Integrations.

Additional details around Okta's developer ecosystem can be located at https://developer.okta.com

Training

Okta offers a wide array of training programs suited to our students' various responsibilities and preferred learning styles. Okta customers can choose from many instructor-led training programs geared towards various roles and education levels. Okta customers can also choose from a variety of self-paced training videos to learn at their own speed or can elect for a private learning experience. Please use our training page (https://www.okta.com/services/training/) to learn more about all the different training programs we offer.

Deployment Assistance

As an Okta partner, Converge Technology Solutions provides professional services and advisory Identity and Access Management (IAM) focused consulting including:

- Consultative services to assist customers with strategic direction, reference architecture, and subject matter expertise on security, identity, risk, compliance, and IT service management.
- Implementation services available to assist customer plan, configure and deploy the Okta service.

- Identity Enablement & Advisory Services to assist our customers in optimizing their Identity Investment by showing how technology capabilities enable their organizational objectives with a multi-year, actionable, decision-centric roadmap.
- Major tasks such as user deployment, application configuration, application integration, Active Directory integration.

Support Plan

Customer success is a core value at Okta, and we pride ourselves on providing an outstanding customer experience. This starts with the way we've designed our product and extends to the way we partner with our customers during and after deployment. Okta offers customer success and support packages that align with the complexity of our customer's environments and provide the critical services needed to achieve business goals with Okta.

The Gold Premier Success Plan offers Okta's fastest technical support and the most personalized level of engagement from a highly knowledgeable account team — who will gain a deep understanding of your business goals and ensure you get the most value from Okta's solutions as your Identity needs grow and evolve.

Training:

- Access to on-demand introductory Okta training
- 20% discount on Public Instructor-Led Training and
- additional on-demand training

Community:

- Grow your skills, connect with peers, and collaborate with our team of product experts

Customer Support:

- 24/7 online and phone support availability
- 30-minute response time for your highest priority cases

Customer Success Services:

- An assigned Customer Success Manager (CSM), who is an Okta Certified Professional and will work with you to develop and achieve a customized success plan for your organization

Technical Resources:

- Access to Technical Account Managers (TAMs), who have deep technical expertise and can provide product-specific technical best practices

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. Okta can integrate with multiple repositories on-premise and in the cloud, and can centralize and link these disparate user stores centrally through Okta's Universal Directory. On-premises, Okta offers direct integrations into Active Directory & v3 compliant LDAP repositories through Okta's Microsoft Active Directory and LDAP Agents.

The Okta Active Directory and LDAP Agents perform the following capabilities:

- Enables the importing of directory user profile information (including custom schemas/attributes) into Okta Universal Directory
- Okta's delegated authentication capability enables organizations to leverage their on-premise Active Directory or v3 compliant LDAP for authentication (without storing credentials in the cloud)
- Enables provisioning user profiles (including custom schemas/attribute) into a Microsoft Active Directory or V3 compliant LDAP directory. This also includes managing directory group memberships and setting user passwords

Okta is able to achieve near real-time account creation and updates. These integrations are established in a variety of ways depending on the system or service Okta is integrating with. As an example, Okta can establish near real-time integrations with solutions that leverage the SCIM provisioning protocol, Rest APIs, or Okta's proprietary connectors which we refer to as "agents" for on-premise directories like OpenLDAP.

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

Okta deploys AD agents to synchronize user identities from on-premise Active Directory to the Okta Cloud Service. These agents (one is sufficient, two or more are recommended) are deployed in an active/active configuration with no primary or secondary agents. As a result, there's no need to proactively load balance agents. All deployed agents are always active and use long polling to constantly look for new jobs as their capacity to handle those jobs allows.

So, instead of Okta waiting for requests from the agent as would happen in a traditional client server relationship, with our long polling model, Okta continually pushes jobs into a job pool and agents grab them as soon as they can. Since jobs get grabbed almost immediately, wait time is eliminated and jobs can be processed faster than would happen with a traditional model.

The Okta AD agent creates an outbound HTTPS connection to the Okta Identity Cloud using certificate pinning with TLS server authentication. Each connection lasts no more than 30 seconds. During that

connection time the AD agent will listen for events from the Okta service that it can process, such as AD authentication events. If such an event appears, the AD agent will grab it for processing and close the connection. The AD agent will then immediately open a new connection and listen again for new jobs. If no events appear during the connection's 30-second window, the agent closes the connection and initiates a new 30-second connection to listen for another job.

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.

Yes, if your passwords are hashed and salted, you can do a bulk import with Okta Users API. Hashing functions supported include SHA-1, SHA-256, SHA-512, BCRYPT, and MD5. However, if your passwords are not salted, or if you do not have the option for a bulk export, you can still migrate a user's password with a just-in-time migration.

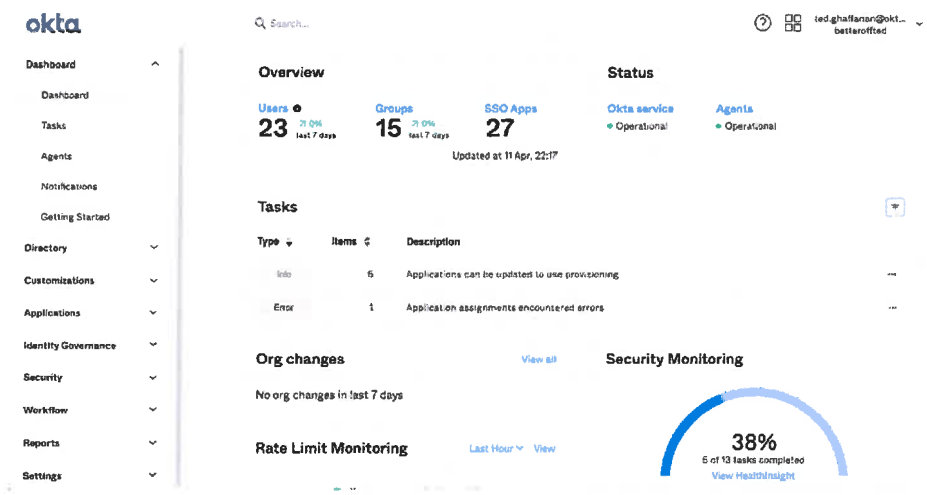
There are several ways to import users and passwords into Okta, but the recommended method is via the Okta Users API. To use the Okta Users API to create a user with a hashed password value you specify a supported algorithm, encrypted password value and the salt used to encrypt that password. These must all be included in the password credential object when creating a user with the Okta Users API. In this method, Okta hashes the hashed password using an Okta algorithm and then finalizes the creation of the new user by setting the user's password.

The complete user migration guide to migrate users from existing user repositories into Okta can be found here:
https://www.okta.com/sites/default/files/pdf/1008_OKTA_User-Migration_Guide_R11101518.pdf

4.3.1.36. Do you have an administrator dashboard User Interface (UI) to manage users? Can you enforce a specific multi-factor type for administrative access?

Yes. The Okta Identity Cloud provides a robust administrator interface (Admin Console) to allow for all administrative functionality including configuration and management of the solution. The Admin Console includes the following tabs that lead to various configuration pages:

- Dashboard
- Directory
- Customizations
- Applications
- Identity Governance
- Security
- Workflow
- Reports
- Settings

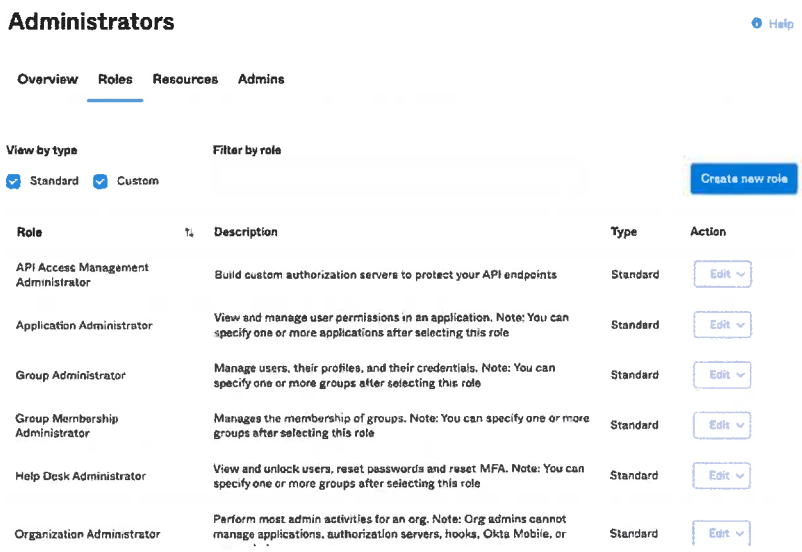


Customers can configure specific step-up MFA rules for Okta administrators. Okta also provides delegated administration capabilities to limit administrator access to specific applications or groups of users.

Additionally, Okta allows organizations to create custom admin roles to fit each unique organizational structure and need, and then subsequently delegate these custom roles to individual users or groups of users where appropriate.

Custom admin roles can be used to create granular roles for admins to manage users, groups, and applications. It provides the flexibility to meet a broad set of use cases while ensuring each admin has just the right level of access they require. For a detailed list, see Okta's support portal:

https://help.okta.com/en-us/Content/Topics/Security/administrators-learn-about-admins.htm



If out of the box Okta delegated administration capabilities are not granular enough to meet your unique business requirements, many customers choose to build their own administrative interface leveraging Okta's Universal Directory/RESTful APIs.

- The Okta Administrator Roles API provides operations to manage administrative Role assignments for a User.
- The Custom Role operations allow for the creation and manipulation of custom Roles as custom collections of permissions.

For more information on how custom roles can be created via API, please visit:
https://developer.okta.com/docs/reference/api/roles/

4.3.1.37. Does the solution support external federation? If so, how, and what Identity Providers (IdPs) are supported?

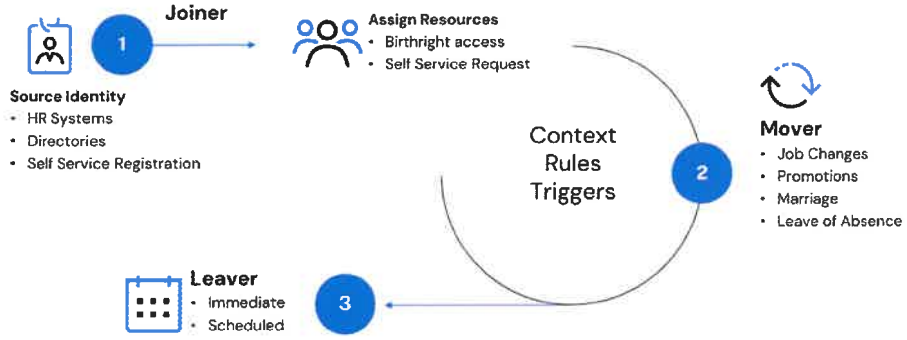
Yes, Okta supports external federation to any IDP that supports open identity standards such as OIDC and SAML. Okta manages connections to other Identity Providers for your application and sits between your application and the Identity Provider that authenticates your users.

You can add connections to social Identity Providers like Apple or Facebook for social authentication. After users authenticate, you sync their existing Identity Provider credentials into Okta Universal Directory while continuing to use that Identity Provider for user authentication. This eliminates the need to store an additional username and password for that user.

You can add connections to Identity Providers that you build in-house that support OpenID Connect or SAML protocols. This is also referred to as Inbound Federation or inbound SAML. The SAML flow is initiated with the Service Provider (in this case, Okta) that redirects the user to the Identity Provider for authentication. After authentication, a user is created inside Okta, and the user is redirected back to your application along with an ID token. This allows you to use Okta to proxy between SAML-only Identity Providers and OpenID Connect-only applications that are normally incompatible.

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

Okta Lifecycle Management streamlines onboarding and offboarding processes by centralizing and automating lifecycle management across all apps on-premise and in the cloud. Users and their devices get instant access to the applications they need, for not a minute longer than they need, while the IT team saves significant management costs.



Lifecycle Management collects all information about a user, including their job title, the groups they belong to, which devices they own, and more from AD, HR, CRM, or ERP systems. Most importantly, the directory is lifecycle aware— a user can be staged, activated, suspended, deactivated, and deleted, based on lifecycle state change events. IT teams can create a self-service flow that sends an app access request directly to the application business owner, like a Sales Director managing Salesforce, who has the best idea of what access level is appropriate. The ticket never touches the IT helpdesk. The following features and capabilities are possible with LCM:

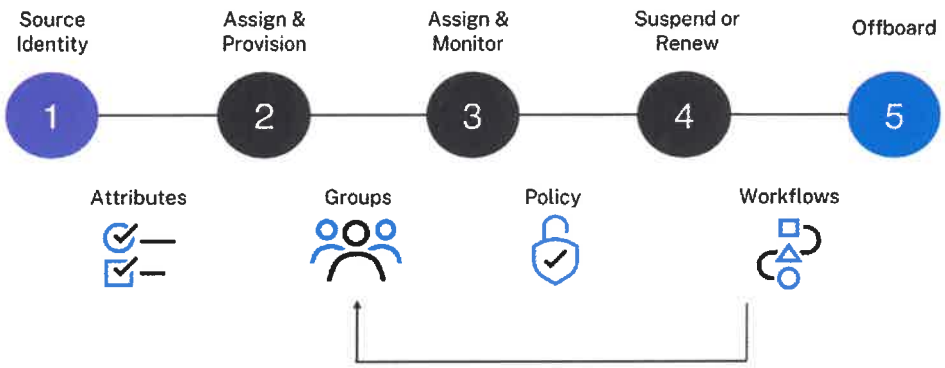
- **Group Membership Rules**: Based on users attributes (e.g. position/department/geography), a user can be automatically assigned to a certain group entitling the user to a certain set of apps and entitlements within the app.
- **App-as-Source**: Pre-integrated provisioning connectors to AD, HRIS, CRM, or ERP applications allowing to source user attributes in Universal Directory, as well as writing back to these applications updates as necessary. Admins can define the priority of the profile sources in Okta.

- **Attribute-Level Sourcing**: The ability to source different user attributes from different authoritative sources (HR, CRM, AD, LDAP, etc.). A user can have his attributes defined by more than one source.

- **Access Request Workflow**: Multi-step self-service access request workflow where users can request any app in the app catalog they don't have, and requests are automatically routed to the appropriate approvers within or outside of IT.

- **Okta Provisioning Agent**: The on-premises provisioning feature extends Okta's provisioning capabilities to on-premises web applications and thick applications that run behind corporate firewalls. Can leverage the SCIM 1.1 standard.

- **Access Reports**: Easily generate reports around app assignment, app access, and deprovisioning of users. Reports can be filtered to focus on certain dates, applications, or users.



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

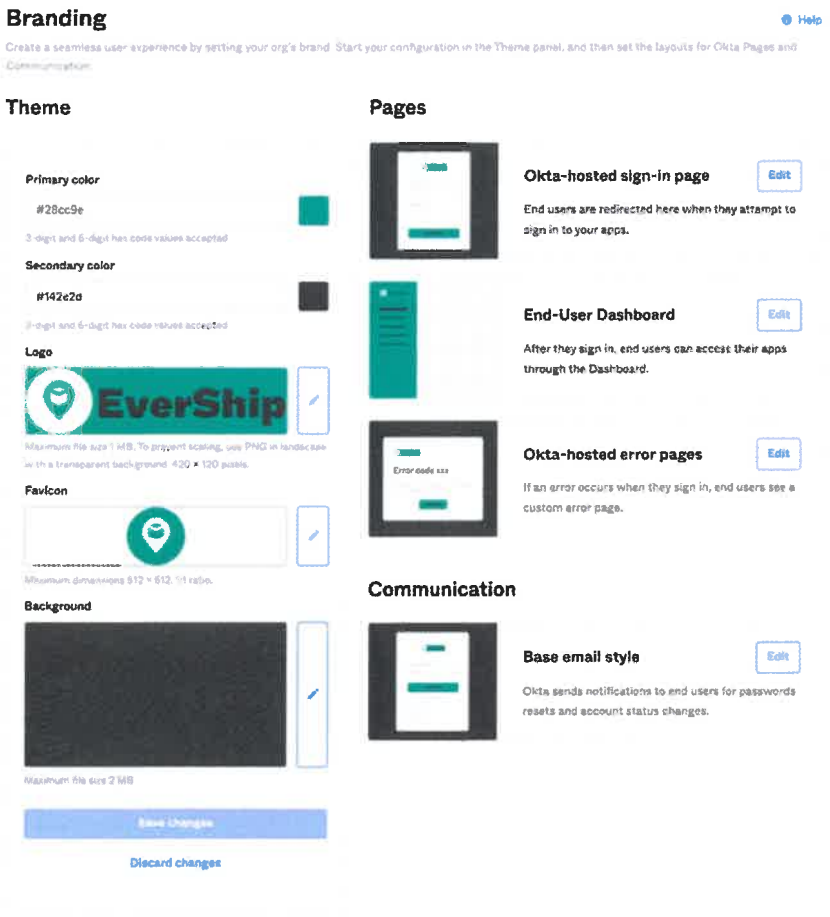
Both Attribute-based Access Control (ABAC) and Role-based Access Control (RBAC) can be achieved by defining Okta Groups with roles. Rules can then be created that auto populate users to certain Role Groups, which then automatically provisions them to applications assigned to that role. Groups are commonly used to assign SSO access within Okta and to provision users to apps with specific entitlements (roles, profiles, etc). When rules are configured to populate groups based on attributes, you achieve ABAC and RBAC.

Okta can also empower ABAC and RBAC within the downstream applications it is authenticating access to. Okta allows admins to customize the attributes passed back to the applications in the SAML assertions or OIDC ID Tokens. These custom attributes can then be utilized by the application in question to customize the experience of the user based on attributes contained in the user's profile within Okta.

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

Admins can customize end-user touch points from a central location in Okta's Admin Console without needing to write custom code. Branding customizes the Okta-hosted sign-in page, including all user authentication flows like registration, MFA, account recovery, consent, factor enrollment, and more. It also controls the Okta end user dashboard, email templates including translated templates, and error pages. Customers create their theme once—including colors, logos, images, styles, and voice—and apply it everywhere at the same time. Customers can also bring their own privacy policy to be used in page footers and remove all mention of Okta for specific use-cases that require whitelabeling.

For more complex branding use cases, Okta also has branding endpoints with SDK support, empowering developers to automate and scale the stack with ease. Customers can either directly call our Brands API or use our suite of Management SDKs to programmatically manage all Okta brand resources at scale. Additional information about our Brands API can be found here:
https://developer.okta.com/docs/reference/api/brands/



4.3.1.41. Are all Multi-Factor Authentication (MFA) factors available for use in authenticating a user prior to performing self-service password maintenance? (E.g., Forgot Password, Change Password, Account Unlock)

Yes. Okta's flexible account recovery feature allows users to reset their password with modern authenticators such as WebAuthn biometrics and Okta Verify Push in addition to email or phone (SMS, voice call). If admins require step up authentication, end users can use any enrolled authenticator. This improves the end user access experience, strengthens security posture, and decreases IT Help desk tickets.

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?

Okta's inline hooks can be configured to call out to custom business logic during an in-flight process (e.g., account registration or authentication) to perform additional activities, such as checking an external password blacklist.

Okta also has a common password detection feature. When end users attempt to set or reset their password that matches a password on this list, they will be prompted to choose a new password. This is enabled via the Common Password Check feature – https://help.okta.com/en/prod/Content/Topics/Security/healthinsight/strong-passwords.htm

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

End-user self-service includes:

- Setting up Okta Mobile to access mobile web apps
- Reset and change Okta or AD/LDAP password from Okta Mobile
- Automated configuration of the devices for corporate services
- Installation of apps from the enterprise app store
- Add/remove personal applications (if enabled)
- Add pre-approved corporate applications
- Request applications that have access request workflow configured
- Configure multifactor authentication
- Customize the tabs and layout of applications in the Okta web app
- View IT notifications
- Edit personal information, such as personal email, phone number for texts or phone verification and forgot password question
- Configure a display language

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

Okta Lifecycle Management supports automatic real-time provisioning and deprovisioning of access based on event-driven identity changes. Okta can automatically provision/de-provision users from items such as Groups/Roles, Application Access, and different policies within Okta using Okta's prebuilt provisioning integrations, Okta Group Rules, and Okta Workflows. Okta's provisioning integrations enable customers to simply "check boxes" to create users, update user attributes, and deactivate users within downstream applications as soon as a user/group is assigned/removed from a given resource in Okta.

With these integrations in place, Okta Group rules automatically detect/trigger on when to automatically provision and deprovision access in Okta based upon a multitude of factors such as user attributes, user group memberships, and other parameters. Not only do Okta Group Rules trigger upon a user's import into Okta, but Group Rules also trigger whenever Okta reads an update made to the user profile from a given authoritative source such as Active Directory, LDAP, Peoplesoft, Workday, etc.

Okta Workflows can also be used to automatically provision and deprovision access based on a plethora of possible events in Okta and other 3rd party applications. Any system event in Okta such as a user activation, user deactivation, user profile updated, or others can be used to drive a provisioning/deprovisioning workflow tailored to specific requirements. More information on Okta events and 3rd Party Application events to trigger automatic provisioning/deprovisioning workflows can be found here: https://help.okta.com/wf/en-us/Content/Topics/Workflows/learn/about-events.htm

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

See 4.3.1.44. Also, customer Okta administrators can manage and end user Okta sessions. Okta also supports Single Logout (SLO) when initiated by a Service Provider (SP). The SP sends the SLO request to Okta to end the Okta session. Okta can support SLO for any app that supports a single logout URL and is integrated with Open ID Connect or SAML federation. Okta SLO is available on an app by app basis, dependent on what the application in question can support.

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?

Yes. All logs can be exported in CSV format only in the current release and can also be pulled in JSON format via read-only RESTful APIs.

There are many methods to ingest Okta System Log events into other systems like Security Information and Event Management (SIEM) solutions, log management tools, and event-driven automation infrastructure. These methods include:

- Log Streaming - Send Okta System Log events to external services in near real-time.
- API polling - Occasionally poll the Okta API to retrieve the latest System Log events.

Note: Many 3rd party tools utilize the Okta API polling to acquire and manage Okta log data. Okta supports the API but does not support 3rd party or open source tooling and integration. However, there are several well known SIEM integrations, as described here: https://support.okta.com/help/s/article/Exporting-Okta-Log-Data?language=en_US

Okta provides APIs that enable integration with best-of-breed SIEM solutions, including ArcSight and Splunk. In addition, Okta has out-of-the-box application integrations with many SIEM solutions to ingest data, including but not limited to the following:

- Splunk
  Splunk customers can leverage a Splunk supported tool to query the Okta API. To obtain the tool, and for usage details, see: https://www.okta.com/integrations/splunk-add-on-for-okta/

- IBM Qradar
  For details, see: https://www.ibm.com/docs/en/dsm?topic=configuration-okta

- SumoLogic
  For details, see: https://github.com/SumoLogic/okta-events

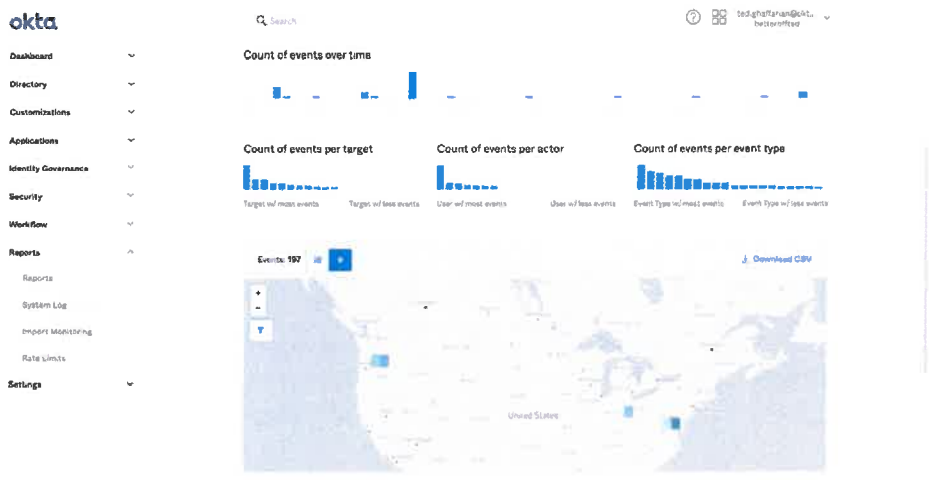
- ELK / ElasticSearch
  For details, see: https://rubygems.org/gems/logstash-input-okta_enterprise/versions/0.1.0
  https://github.com/SecurityRiskAdvisors/logstash-input-okta_enterprise

- Rapid7
  For details, see: https://docs.rapid7.com/insightidr/okta/

- LogRhythm
  For details, see: https://docs.logrhythm.com/docs/devices/api-log-sources/api-okta-event

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.

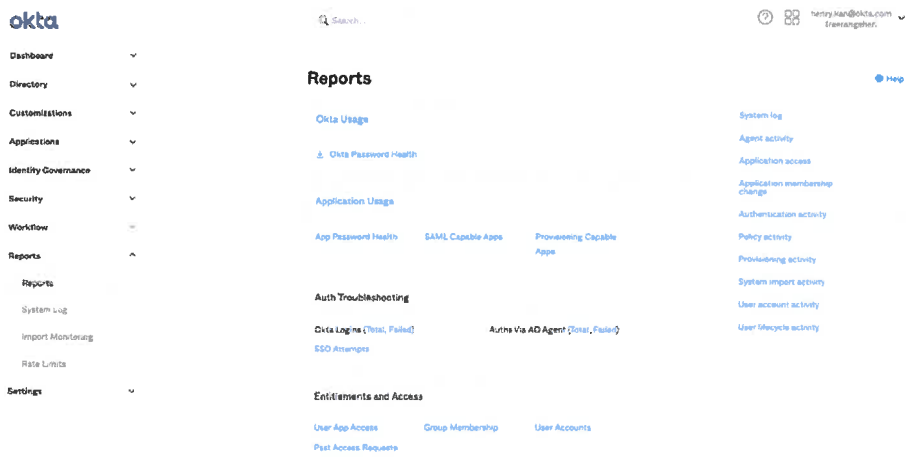
Yes. Okta offers the ability to filter system log data in real-time via a graphical admin interface. Administrators, including data owners, can save advanced filters as custom reports, which can be rerun on-demand. Data can also be accessed via an API and exported for use in third party systems.



Okta stores 40+ metadata attributes, including user attributes and contextual data, about every event that occurs in the system. Okta also has numerous built in reports including but not limited to:

- Agent Activity
- Application Access
- Application Membership Change
- Authentication Activity
- Policy Activity
- Provisioning Activity
- System Import Activity
- User Account Activity
- User Lifecycle Activity

The data underlying these reports can all be exported in .CSV format directly from the admin console in Okta's service.

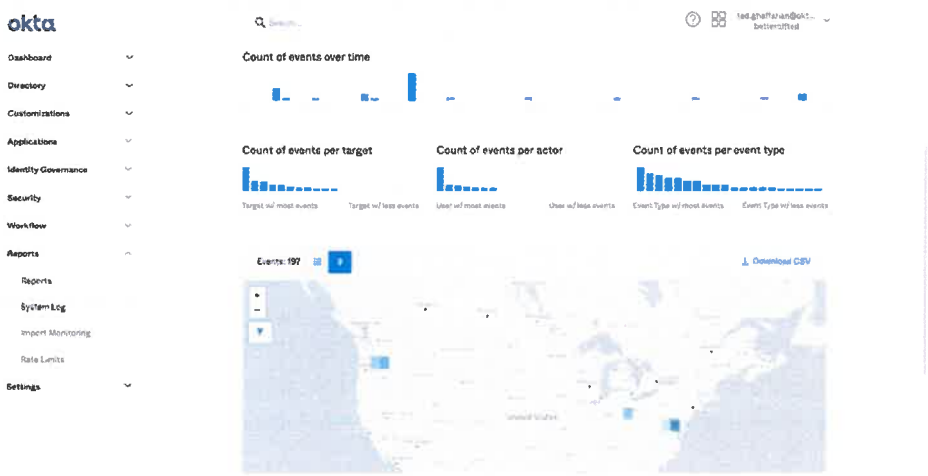


4.3.1.48. How long are the logs maintained?

Customer application logs are kept for 3 months - see Okta's data retention policy https://support.okta.com/help/s/article/Okta-Data-Retention-Policy which provides details on how log data can be exported and integrated with customer's SIEM for longer retention (https://support.okta.com/help/s/article/Exporting-Okta-Log-Data).

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

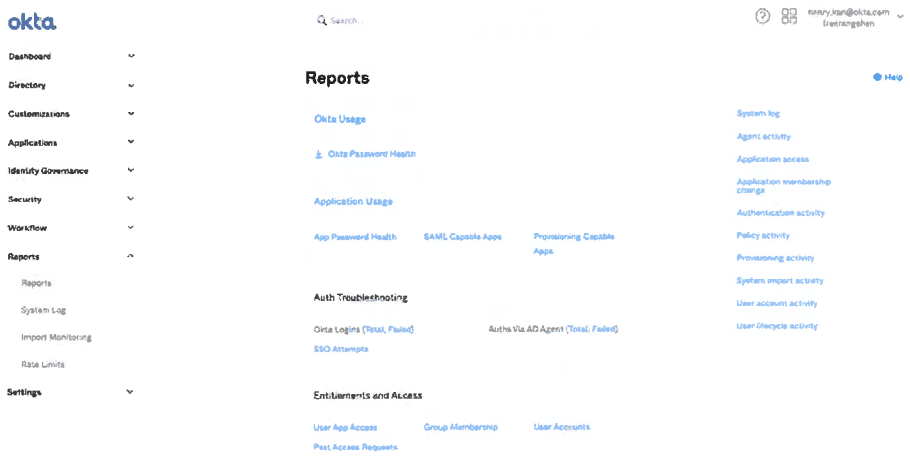
Yes. Okta offers the ability to filter system log data in real-time via a graphical admin interface. Administrators, including data owners, can save advanced filters as custom reports, which can be rerun on-demand. Data can also be accessed via an API and exported for use in third party systems.



Okta stores 40+ metadata attributes, including user attributes and contextual data, about every event that occurs in the system. Okta also has numerous built in reports including but not limited to:

- Agent Activity
- Application Access
- Application Membership Change
- Authentication Activity
- Policy Activity
- Provisioning Activity
- System Import Activity
- User Account Activity
- User Lifecycle Activity

The data underlying these reports can all be exported in .CSV format directly from the admin console in Okta's service.



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

Okta logs industry-standard events as defined by US FedRAMP & NIST standards, including, but not limited to: successful / failed logins, successful / failed connection attempts, privileged user access and activities, processes, object accesses. Log entries include applicable information such as date/time, event type, message, outcome or actions, userID or account, source / destination IP, port, protocol, and other relevant information. For more information, please see: https://developer.okta.com/docs/reference/api/system-log/

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

For the Okta application, customers use their Okta administrative console to access the application logs. For the infrastructure logs, Okta uses Splunk to collect logs from various sources, such as the Okta application and our systems in AWS. Okta has its own security-related correlation rules to detect and analyze potential security events, which are monitored and reviewed regularly by the security team. All logs are kept encrypted in AWS. Infrastructure logs (firewall/IDS) are kept for 1 year.

Customer application logs are kept for 3 months - see Okta's data retention policy which provides details on how log data can be exported and integrated with customer's SIEM for longer retention: https://support.okta.com/help/Documentation/Knowledge_Article/Okta-Data-Retention-Policy

All communication between Okta and the customer is protected by TLS 1.2 capable services supporting Perfect Forward Secrecy (PFS) and AES 256-bit encryption. We also utilize HTTP Strict Transport Security (HSTS) which prevents the down-grade of HTTPS communication to clear-text HTTP.

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

Okta's reporting engine is built to enable administrators to view system activity in real time, and on demand. Okta provides system log event data in real time via a graphical user interface (dashboard), and RESTful APIs as well as a CSV export. Okta stores 40+ metadata attributes, including user attributes and contextual data, about every event that occurs in the system.

Okta provides APIs which enable integration with Business Intelligence products for SIEM and real time compliance reporting and alerting purposes. In addition, Okta has out of the box application integrations with some business intelligence products, including Splunk

Okta provides various ways to ingest data to Security Information and Event Management (SIEM) solutions.

Alerts can also be automated through Okta Workflows' pre-built capability to send notification emails out to defined administrators or groups of administrators.

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

Yes. Okta's reporting engine is built to enable administrators to view system activity in real time , and on demand. Okta provides system log event data in real time via a graphical user interface, and RESTful APIs as well as a CSV export. Custom audit trails and activity reports can be set to run on a cadence and workflows can be configured to send reports to specified administrators.

4.3.1.54. What options are available for exporting logs and reports to external systems or Security information and event management (SIEM) solutions?

Okta provides APIs that enable integration with best-of-breed SIEM solutions, including ArcSight and Splunk. In addition, Okta has out-of-the-box application integrations with many SIEM solutions to ingest data, including but not limited to the following:

- Splunk
  Splunk customers can leverage a Splunk supported tool to query the Okta API. To obtain the tool, and for usage details, see: https://www.okta.com/integrations/splunk-add-on-for-okta/

- IBM Qradar
  For details, see: https://www.ibm.com/docs/en/dsm?topic=configuration-okta

- SumoLogic
  For details, see: https://github.com/SumoLogic/okta-events

- ELK / ElasticSearch
  For details, see: https://rubygems.org/gems/logstash-input-okta_enterprise/versions/0.1.0
  https://github.com/SecurityRiskAdvisors/logstash-input-okta_enterprise

- Rapid7
  For details, see: https://docs.rapid7.com/insightidr/okta/

- LogRhythm
  For details, see: https://docs.logrhythm.com/docs/devices/api-log-sources/api-okta-event

There are many methods to ingest Okta System Log events into other systems like Security Information and Event Management (SIEM) solutions, log management tools, and event-driven automation infrastructure. These methods include:

- Log Streaming - Send Okta System Log events to external services in near real-time.
- API polling - Occasionally poll the Okta API to retrieve the latest System Log events.

Note: Many 3rd party tools utilize the Okta API polling to acquire and manage Okta log data. Okta supports the API but does not support 3rd party or open source tooling and integration. However, there are several well known SIEM integrations, as described here: https://support.okta.com/help/s/article/Exporting-Okta-Log-Data?language=en_US

4.3.1.55. Indicate and identify any countries where you provide services to clients outside of the United States (and US territories).

Okta has over 18,800 customers both within the United States and around the world. For a comprehensive list of Okta's publicly referenceable customers, please see: https://www.okta.com/customers/

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.

Any reportable security breach would be included in Okta's current public filings available at https://investor.okta.com/

Okta also publishes a public-facing blog that is regularly updated with detailed information about any security incidents, analyses, and remediations: https://sec.okta.com/articles

Please also see Okta's Secure Identity Commitment: https://www.okta.com/secure-identity-commitment/

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

Our deployment process has been architected to support continuous delivery with zero downtime for service updates.

Weekly and monthly releases are made to the service and include risk-based patching. Typically, weekly releases will contain only fixes while monthly releases will contain new features and changes to existing features.

Each release includes a release notes document that describes the patch, features, and other service updates: https://help.okta.com/oie/en-us/content/topics/releasenotes/oie-relnotes.htm

4.3.1.58. Where does the solution reside?

Amazon Web Services (AWS) provides the infrastructure that hosts Okta's identity-as-a-service platform (IDaaS). The data center locations for AWS (and other sub-processors) are listed in Okta's Sub-processor Information document, available at https://www.okta.com/trustandcompliance/.

Okta stores Customer Data at rest in the geographic region of the cell purchased by the customer (i.e., for the State of West Virginia, all data would stay in North America).

- In North America, Okta uses multiple availability zones in AWS data centers located in Virginia, Ohio, and Oregon.
- In Europe, data are located in AWS's Dublin, Ireland with backup operations in Frankfurt, Germany.
    - PLEASE NOTE: Customer EU orgs onboarded prior to June 1, 2019, primary is in Germany and backup/failover is in Ireland.
- In Asia-Pacific, data are located in AWS Sydney, Australia with backup operations in Singapore.
- In Japan, data are located in AWS Tokyo with backup operations in Osaka.

Exact physical location of these facilities are kept secret by Amazon. Amazon publishes the following information on their data center locations: https://aws.amazon.com/about-aws/global-infrastructure/

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.

Okta's mission is to connect any user to any technology. We design, develop, and test our products with accessibility in mind so that all users can use our products, including users with disabilities, such as visual impairment, color deficiency, and hearing impairment.

For more information and copies of our Voluntary Product Accessibility Template (VPAT) by our third-party auditors (Level Access and Deque), please see: https://www.okta.com/accessibility/

The Okta Sign-in Widget and the Okta End User Dashboard conform to WCAG 2.1 AA specification (a part of Section 508) in a partially or fully supports conformance level as certified by outside auditor, Deque.

The Okta Verify app and the Okta browser plugin conform to WCAG 2.0 AA specification (a part of Section 508) in a partially or fully supports conformance level as certified by outside auditor, Level Access.

We are currently in the process of formally assessing our 508 compliance to address gaps in our support. In the meantime, we try to address specific 508 compliance issues when identified by customers. In a B2C use case, customers build their own applications leveraging Okta's comprehensive RESTful APIs. The custom built applications can built to meet the customers requirements. Additional information regarding the Okta developer ecosystem can be found at https://developer.okta.com.

4.3.1.60. Describe how your service provides failover and redundancy.

Okta has formally documented procedures to be used when responding to an unplanned business interruption.

The primary objective of Okta's BCP is to respond safely, effectively, and efficiently to any emergency that has the potential to impact our staff or our business with an emphasis on retaining Information Security

controls during and after the incident. This plan acts as Okta's Emergency Response Plan (ERP), Okta's Business Resumption Plan (BRP), Okta's Crisis Management Plan (CMP), and Okta's Pandemic Response Plan (PRP). BCP is tested annually.

Okta maintains regional and geographical disaster recovery capacity and has formally documented DR standard operating procedures. If one zone is down, Okta is able to quickly use another zone for continuous operation. DR is tested quarterly. The service's DR and BC components are audited and attested to within Okta's Workforce and Customer Identity cloud SOC2 Type II report. Okta's BCP documentation is made available to prospects under NDA.

NOTE: Disaster Recovery (DR) is tested quarterly. It is a full failover test and has no impact on customers. Okta's SOC2 Type II report attests to our quarterly successful DR testing.

A list of all service certifications and compliance reports is available at https://trust.okta.com/compliance/

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

Okta uses AWS Shield Advanced for application-wide DDoS detection and protection against layer 3 and 4 infrastructure attacks and application layer attacks like HTTP floods.

Details here: https://aws.amazon.com/shield/ddos-attack-protection/

Okta also uses AWS WAF for automatic filtering based on IP address, geographic blocking, or information available in the HTTP headers. Additional AWS protections are currently being evaluated as part of our continuous improvement efforts to protect the Okta service.

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

Okta runs on an enterprise-grade architecture that is multi-tenant, and runs with extremely high availability (99.99%) and scalability.

The Okta service is built on an on-demand cloud architecture. Our highly differentiated cell architecture is a self-contained instance of the entire Okta service. Each cell has its own set of Job/Database servers, Load Balancers and App Servers and is capable of hosting user identities independent of other cells. Okta spins up additional cells as needed, with each having its own complete high availability, high performance architecture to help scale the system and host additional users if the need arises. Okta's service and operations are specifically designed to scale against demand for users (on-boarding new identities) and concurrent usage (# of user Authentications) which allows Okta to onboard large customers in a predictable and scalable fashion.

Okta's High Availability Architecture is described here:
https://www.okta.com/sites/default/files/2022-09/Okta%20High%20Availability%20Architecture_Whitepaper.pdf

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

Okta has a defined Disaster Recovery Plan:

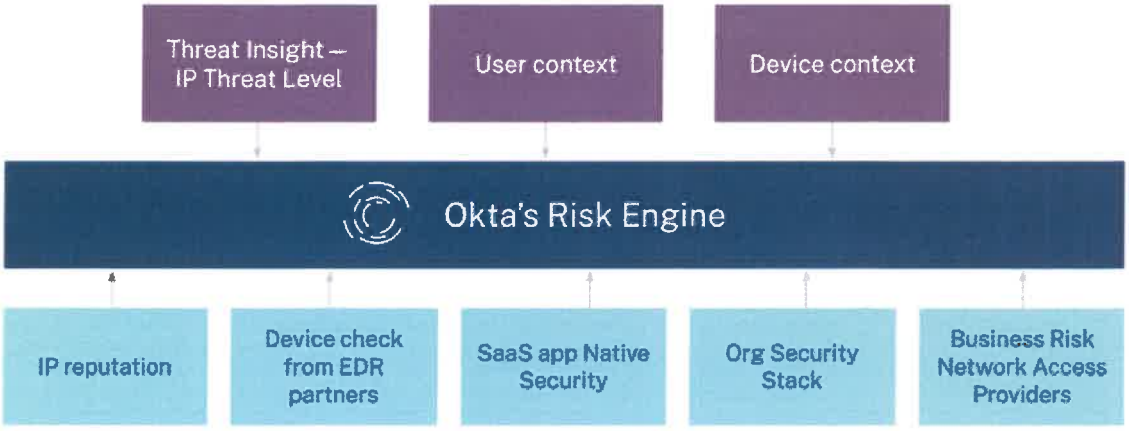
1) During an incident response or disaster recovery, Okta personnel's primary goal is to restore full service functionality and availability as soon as possible. Additionally, it is the goal of Okta personnel to protect sensitive and proprietary data according to Okta policies and procedures, legal requirements, and any specific client requirements. Sensitive data includes, but is not limited to: personal information of users for the Okta service, login IDs or passwords of users or internal employees, all data stored in customer supported databases and Okta intellectual property (software codes, etc.). Okta's Incident Response & Disaster Recovery SOP is shareable on request under NDA.

2) Okta takes advantage of EC2's ability to place instances within multiple geographic regions, as well as across multiple availability zones. Each availability zone is designed with fault separation. Availability zones are physically separated within a typical metropolitan region, on different flood plains, in seismically stable areas. In addition to discrete, uninterruptable power sources and onsite backup generation facilities, each availability zone is fed through different grids from independent utilities to further reduce single points of failure. All availability zones are all redundantly connected to multiple tier-1 transit providers.

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

Okta assigns a risk level to each Okta sign-in using models that use contextual information about the sign-in as well as historical information about the user. Admins can configure a sign-in policy rule to take different actions based on the risk level of the sign-in. For example, prompt for MFA if the login is high risk. Admins can create a sign-on policy rule, set a risk level, and assign a corresponding action based on the specified risk level. A high risk is assigned to new users initially — over time the risk level is reduced as more information is gathered about the user's login pattern. Over time, the risk associated with normal sign-ins for the user will decrease. Risk Scoring is designed to complement, not replace existing security tools and should not be used to:

- Substitute bot management or automation detection
- Replace Web Application Firewalls (WAFs)
- Assist with any type of security compliance



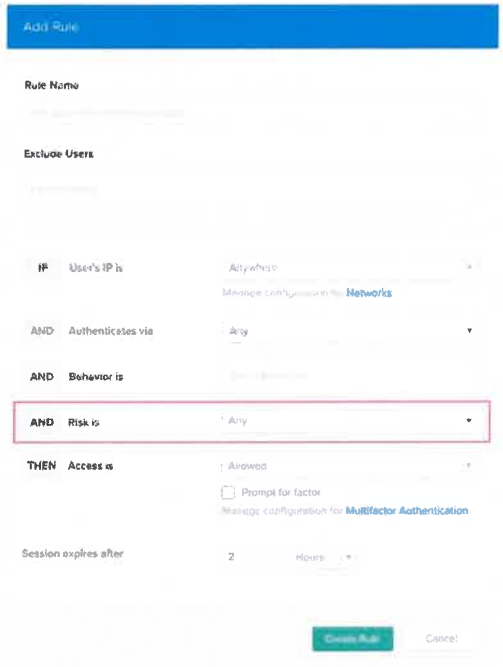
System Log events

System logs contain risk information associated with authentication. The System log provides insights into how the risk was determined including any combination of the following reasons:

- Anomalous Location
- Anomalous Device
- Suspected Threat (based on Okta ThreatInsight detection)

Configure Risk Scoring

Configure Risk Scoring by adding a rule and configure the risk level for the rule.



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

Okta enables customers to leverage threat intelligence that we have aggregated from across the platform via ThreatInsight.

Okta ThreatInsight aggregates data about sign-in activity across the Okta customer base to analyze and detect potentially malicious IP addresses and to prevent credential-based attacks such as:

- password spraying
- credential stuffing
- brute-force cryptographic attacks

Because ThreatInsight collects information about the origin of sign-in activity directed at Okta organizations and Okta endpoints, it provides a security baseline for all Okta customers. You can choose to log events for auditing or to log events and block traffic that ThreatInsight has identified as suspicious. If you choose to log and block traffic, Okta automatically denies access to sign-in requests that come from potentially malicious IP addresses that ThreatInsight has detected.

Okta Threat Insight allows Okta customers to build policies based on risk signals seen across Okta's global data-set, such as high-risk IP addresses. As we add more identities to our platform, we gain increasingly valuable insights about our users, their devices, their location, the applications they access, where security attacks are originating, and much more. We use the data to understand usage trends and predict customer

needs, driving product innovation and new feature development that enriches our offerings and improves security.

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

Okta controls attributes through the Universal Directory, where attributes are set to READ-WRITE, READ-ONLY, and HIDDEN to an individual's User Profile. Okta's robust cloud-based directory service, Universal Directory, enables organizations to integrate with multiple identity stores simultaneously, including Active Directory, V3-compliant LDAP directories, and third-party human resources management systems (HRMS) solutions (e.g., Workday, PeopleSoft, Custom HR/User Store Databases.)

User attributes can only be modified by Okta administrators with the right set of permissions. Any changes to user attributes are also recorded in Okta's system log.

Every attribute in the user schema has permission configurations that allows Admins to decide whether end users or other admin roles are able to read and/or modify an attribute. End users can then manage their profile through an out of the box interface.

Okta also supports Attribute Mastering, where a single Identity Source can control a single or multiple attributes in a user profile, which would then prevent changes to that attribute from other sources, marking it 'Read-Only'.

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

Okta provides a group-based sign-on policy to manage global session lifetime (idle and max) for the access manager that can be conditional on network location/geo of the client. Okta does not support application-level session tracking, but instead provides the option to configure app-level sign-on policies to define time/device session assurance requirements and step-up re-authentication. Administrators can end all sessions for a user via the Admin Console or API and can end specific sessions for a user via API.

Okta also provides an OAuth 2.0 Authorization Server that can define access token and refresh token lifetimes for specific OAuth clients and grant_types.

4.3.1.68. Are sessions cleared upon logging off?

Okta supports Single Logout (SLO) when initiated by a Service Provider (SP). The SP sends the SLO request to Okta to end the Okta session. Okta can support SLO for any app that supports a single logout URL and is integrated with Open ID Connect or SAML federation. Okta SLO is available on an app by app basis, dependent on what the application in question can support.

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

Yes. Administrators can end all sessions for a user via the Admin Console or API and can end specific sessions for a user via API.

4.3.1.70. Describe your approach to managing long-running sessions

The session timeout in Okta is fully customizable. The default session timeout in Okta is 2 hours, but it can be set to as little as 1 minute or up to several hours or days for certain use cases.

4.3.1.71. How does your platform manage user sessions in scenarios where users access applications from various locations?

Users can access applications for different locations. However, Okta's AMFA would leverage a number of user contexts to determine impossible travel or suspicious activity, requiring step-up authentication.

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

Administrators can end all sessions for a user via the Admin Console or API and can end specific sessions for a user via API.

4.3.1.73. Does your solution integrate with Active Roles Server?

Yes, Okta integrates with Active Roles via Secure Web Authentication today, and Quest will be supporting SAML authentication in an upcoming release which will allow SSO and MFA from Okta.

4.3.1.74. Explain how your platform complies with industry standards and regulations related to data security and privacy.

As the leader in cloud Identity and Access Management, our business is based on the secure storage of PII. To help demonstrate this, Okta maintains certification in SOC2 Type II (was SAS70), ISO 27001, ISO 27017, ISO 27018, and Cloud Security Alliance STAR Attestation / Level 2.

Okta is FedRAMP Moderate and FedRAMP High certified.

Okta is the first Identity-as-a-Service product to obtain CSA STAR Level 2, requiring independent 3rd party review of the effectiveness of our security controls compared to the requirements defined in the CSA Cloud Guidance. The CSA STAR program is built upon the Cloud Security Alliance Cloud Controls Matrix, a controls

framework tied to international standards such as ISO and SOC, but focused on cloud-specific requirements.

Okta is also HIPAA compliant.

All of the aforementioned certifications, including links, are always available at: https://trust.okta.com/compliance

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. The vendor must provide the three references upon request but must e provided prior to contract award.

Okta has provided the contract information for three current customers with similar requirements and similar or larger user bases. Out of respect for our customers' privacy, Okta cannot provide a current user count range. However, once Okta has been shortlisted for a more thorough evaluation, we are happy to facilitate introductions to a few of our reference customers.

State of Delaware
Navin Singhal
Technology Senior Manager
Department of Technology and Information, State of Delaware
navin.singhal@delaware.gov
973-979-2500

Commonwealth of Kentucky
Phil St. John
Assistant Director
Division of Information Management
Department of Revenue
Finance and Administration Cabinet, Commonwealth of Kentucky
phil.stjohn@ky.gov
502-330-1984

State of Iowa
Darwin Ten Haken
ITEE Enterprise Architect, State of Iowa
darwin.tenhaken@iowa.gov
515-226-9756

4.4. Mandatory Qualification/Experience Requirements

The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

4.4.1.1. Vendor must provide SSAE No. 18 SOC 1 Type 2 report results yearly to satisfy overall State of WV SOCI requirements.

Converge has wholly owned subsidiaries that maintain SOC 1 Type 2 and SOC 2 Type requirements.

Acknowledgement of Addendums

Following this page, please find the signed addendums.

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
Doc Description:	Identity Management Single Sign-On Solution
Proc Type:	Central Master Agreement
Reason for Modification:	To post addendum 01.

Date Issued	Solicitation Closes	Solicitation No	Version
2024-03-05	2024-03-26 13:30	CRFP 0947 ERP2400000002	2

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: VS0000041625
Vendor Name : Converge Technology Solutions US LLC
Address : 130
Street : Technology Parkway, Suite 100
City : Peachtree Corners
State : GA **Country :** USA **Zip :** 30092
Principal Contact : Charlie Arnett
Vendor Contact Phone: 304-549-7698 **Extension:**

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

Vendor Signature X DocuSigned by: karen Smallwood FD6598FB840A4D2... **FEIN#** 82-2782457 **DATE**

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

ADDITIONAL INFORMATION

Addendum 01:
1. To extend the bid opening from March 12, 2024 to March 26, 2024. The bid opening time still remains at 1:30PM EST.

2. Responses to vendor questions will be issued under a separate addendum.

INVOICE TO	SHIP TO
ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US	ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	See Exhibit A - Pricing Page				

Comm Code	Manufacturer	Specification	Model #
81112501			

Extended Description:
See attached documentation for complete details.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Vendor Technical Questions due by 2:00PM EST	2024-03-01

SOLICITATION NUMBER: CRFP ERP24*02
Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[✓] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

1. To extend the bid opening from March 12, 2024 to March 26, 2024. The bid opening time still remains at 1:30PM EST.

2. Responses to vendor questions will be issued under a separate addendum.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP ERP24*02

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[x] Addendum No. 1	[ ] Addendum No. 6
[x] Addendum No. 2	[ ] Addendum No. 7
[ ] Addendum No. 3	[ ] Addendum No. 8
[ ] Addendum No. 4	[ ] Addendum No. 9
[ ] Addendum No. 5	[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

VS0000041625
Company

DocuSigned by:
karen Smallwood
FD6598FB840A4D2...
Authorized Signature

4/2/2024
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

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			To post addendum 02.
Proc Type: Central Master Agreement			
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2024-03-20	2024-04-04 13:30	CRFP 0947 ERP2400000002	3

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: VS0000041625
Vendor Name : Converge Technology Solutions US LLC
Address : 130
Street : Technology Parkway, Suite 100
City : Peachtree Corners
State : GA **Country :** USA **Zip :** 30092
Principal Contact : Charlie Arnett
Vendor Contact Phone: 304-549-7698 **Extension:**

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

Vendor Signature X DocuSigned by: Karen Smallwood FD6598FB840A4D2... **FEIN#** 82-2782457 **DATE** 4/2/24

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

ADDITIONAL INFORMATION

1. To post answers to vendor questions.
2. To attach Exhibit B - State of WV Unique Login History.
3. To attach WV Software As a Service Addendum
4. To extend the bid opening from March 26, 2024 to April 04, 2024. The bid opening time still remains at 1:30PM EST.

No other changes.

INVOICE TO	SHIP TO
ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US	ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	See Exhibit A - Pricing Page				

Comm Code	Manufacturer	Specification	Model #
81112501			

Extended Description:
See attached documentation for complete details.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Vendor Technical Questions due by 2:00PM EST	2024-03-01

SOLICITATION NUMBER: CRFP ERP24*02
Addendum Number: 2

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[✓] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[✓] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[✓] Other

Description of Modification to Solicitation:

1. To post answers to vendor questions.

2. To attach Exhibit B - State of WV Unique Login History.

3. To attach WV Software As a Service Addendum

4. To extend the bid opening from March 26, 2024 to April 04, 2024. The bid opening time still remains at 1:30PM EST.

No other changes.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

Vendor Questions – CRFP ERP24*002

March 4, 2024

1. Please confirm our assumption that users of this system in the future state timeframe (3 years) are internal workforce type users(employees, contingent workers) and not the public.

    a. Both, currently wvOASIS does not identify a difference between employees and citizens.

2. Some applications listed for integration included CGI Advantage, UKG, Deighton, and others. Do all the in-scope applications support integration through a modern protocol like SAML or OIDC?

    a. The service we are requesting should be able to handle multiple applications simultaneously and allow wvOASIS to add and remove applications as needed.

3. Can you please share the details of any applications that require alternative mechanisms and those mechanisms?

    a. Not Applicable, the vendor needs to provide all the solutions that can be provided as part of their proposal.

4. There is not a significant focus on assistance in migrating from MyApps to the future state platform. (outside of Q4.3.1.32) What level of services support does WV desire for this initiative?

    a. This is being requested as a SaaS solution. The vendor should indicate their platform's capabilities. The pricing sheet indicates our estimate for expected hours.

5. Please provide clarification on the RADIUS requirement being cloud delivered.

    a. Per section 4.3.1.8 the agency is asking a yes or no question to whether or not the vendor's solution provides RADIUS support without on-premise components.

6. May we please get a two-week extension to respond to the bid?

    a. The bid opening date has been extended from March 26, 2024 to April 04, 2024. The bid opening time still remains at 1:30PM EST.

7. How many environments are currently available in the MyApps custom Identity management solution?

    a. The service we are requesting should be able to handle multiple applications simultaneously and allow wvOASIS to add and remove applications as needed. We are requesting a solution that can add and remove an unlimited number of environments.

8. How many environments for the new SSO platform (e.g., Development, Production, etc.) are planned/required for this initiative?

    a. The service we are requesting should be able to handle multiple applications simultaneously and allow wvOASIS to add and remove applications as needed.

    We are requesting a solution that can add and remove an unlimited number of environments.

9. Please provide a list of the applications that are currently integrated with the legacy platform.

    a. The service we are requesting should be able to handle multiple applications simultaneously and allow wvOASIS to add and remove applications as needed.

    Applications are subject to change and need to be able to be added/removed by the client.

10. Are there additional applications in scope to be migrated to the new SSO platform?

    a. The service we are requesting should be able to handle multiple applications simultaneously and allow wvOASIS to add and remove applications as needed.

    We are requesting a solution that can add and remove an unlimited number of environments.

11. Please provide the list of on-premises applications that will be integrated with the new IAM solution for SSO.

    a. The service we are requesting should be able to handle multiple applications simultaneously and allow wvOASIS to add and remove applications as needed.

       We are requesting a solution that can add and remove an unlimited number of environments.

12. Please provide the list of cloud-based applications that will be integrated with the new IAM solution for SSO.

    a. The service we are requesting should be able to handle multiple applications simultaneously and allow wvOASIS to add and remove applications as needed.

       We are requesting a solution that can add and remove an unlimited number of environments.

13. Do we need to migrate the existing user access data (such as roles and permissions) from the legacy system to the new SSO platform as part of the user data migration? If the answer is yes, please let us know which system (such as a database or an LDAP) is hosting this information.

    a. No

14. Are there any expectations of integration with the MyApps custom Identity management solution?

    a. No

15. What types of users (e.g., employees, contractors, citizens, business partners) and how many are in scope for migration to the new SSO platform? Additionally, what is the system of record for each user type?

    a. Both, currently wvOASIS does not identify a difference between employees and citizens. We don't intend to require a different designation between types of users. A user is a user.

16. Please let us know which capabilities from the legacy MyApps Identity Management system are in scope for migration to the new SSO platform. Examples of capabilities include SSO, MFA, IGA (user lifecycle management), application provisioning, and password management.

    a. Not Applicable. We are intending to implement an entirely new solution separate from our legacy system.

17. Regarding the support for the proposed SSO platform (not the product support or warranty), will the support be expected from the vendor? If so, what is the expected duration and support model - 24*7 or 8 by 5?

    a. Yes, support is expected. 24/7.

18. Is the use of offshore staff (located outside the US) allowed for implementation or support services?

    a. Yes

19. Can a vendor submit more than one proposal response with different SSO vendors?

    a. Yes, a separate proposal is required for each proposal. If submitting more than one proposal, please identify with Proposal 1, Proposal 2, etc., to avoid confusion and to eliminate the possibility it may be viewed as a duplicate.

20. Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below
    Are these requirements 'hard' requirements or, as this line suggests, are some of them simply 'desirable' but optional?

    a. This is a desirable

21. 4.3.1.11 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

    4.3.1.12 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.

    Please verify that these items address the same requirement.

    a. These are two separate questions. We encourage the vendor to answer each question as stated.

22. 4.1.1.31 Do you offer flexible application integrations such as general Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and Open Authorization (Oauth) connectors?

    Previous bullets failed to include a req for OAuth. Is OAuth a requirement or not?

    a. We were providing the vendor with examples, we are asking the vendor to provide authentication methods that are supported.

23. 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?

    Is this a requirement ONLY for newly submitted passwords or do existing passwords need to be evaluated against known compromised passwords?

    a. Newly submitted passwords only.

24. 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.

    Like WV, many customers do not want their information shared in a public forum. Is it acceptable to provide references in a less public arena?

    a. This section will be revised so the Vendors three references is not required with their bid response. However, Vendors must provide three references upon request but must be provided prior to contract award.

       Original specification Section 4.3.1.75. is now deleted.
       Specification Section 4.3.1.75. is now revised to say:
       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. The vendor must provide the three references upon request but must be provided prior to contract award.

       Vendor should review the following sections of the terms and conditions:
       section 30 - Privacy, Security, and Confidentiality,
       section 31 – Your Submission is a Public Document.

       Lastly, the vendor's submission is subject to Freedom of Information Act (FOIA).

25. What user data export options are supported with Ultimate Kronos Group? (ie CSV, SCIM, etc.)
    a. Not Applicable. This application will not have users exported from UKG.

26. How often should these changes be synchronized to the new identity management solution?

    a. Not Applicable. The solution will not be synchronizing with the applications. Users will need to be synced out of band from the SaaS Identity Management Solution.

27. In order for us to provide the best possible response to the State, please provide a two-week extension to the proposal date.

    a. Please see answer to question number #6

28. Would the state consider granting a 2-week extension to the 03/12 due date to allow us more time to respond properly?

    a. Please see answer to question number #6

29. Exhibit A – Pricing Page. Will the state be paying for years 1-3 upfront in year 1? Or is the expectation for a 3 year commitment with annual invoicing?

    a. The expectation is for a 3-year commitment with annual invoicing.

30. Cost evaluation and scoring. Will the cost scoring be based on the total cost of years 1, 2 and 3?

    a. The evaluation process will encompass the entire 6 years (initial 3 years plus 3 – 1-year extensions) of the contract.

31. The 24,000 unique logins per month user count aligns with a CIAM consumption model. Can you share the total number of registered users?

    1. *Exhibit A – Pricing Page: SAAS Software License - Pricing to reference both unique and total logins for the calendar year 2023 as attached. This is not referencing named or assigned user accounts. Average of 24,000 Unique Logins per month*

    a. This is being provided as an addendum.

2. An attachment is referenced but we do not believe the attachment was included in the RFP. Can you please provide the attachment?

    a. Yes, see attached document titled Exhibit B - State of WV Unique Login History

32. Can you please provide as soon as possible word versions of the documents, especially the technical/project requirements portion?

    a. No, an editable version will not be provided.

33. "Vendor must provide contact information for each reference and current user count range. The estimated range should be greater than 30,000 users." - What type of users are these (employees or citizens)?

    a. Both, currently wvOASIS does not identify a difference between employees and citizens. Roles are to be assigned internally.

34. Are Citizens ever going to be in scope on this platform?

    a. Yes

35. Any plans to add Identity Governance use cases for employees?

    a. The vendor may suggest and provide options, however if the RFP does not state this specifically there is no need to respond.

36. Can you provide the application protocols used in your applications? SAML, OAUTH, etc.

    a. No, the reason is that we are planning on changing some of the protocols as part of this project that will not involve any work from the vendor. The vendor must simply be able to propose the standard protocols they provide as part of their solution in the RFP.

37. Are there any legacy applications in scope? E.g. Mainframe. ERP, header injection applications?

    a. Legacy can take on a large scope of possibilities. The vendor needs to reply with the proposed solution that best fits the requirements.

38. Is a GovCloud a requirement?

    a. No

39. Does the state have plans to deploy components on-premise along SaaS? For example, is there a need to have LDAP on-premise and IAM in SaaS?

    a. The proposal being requested is in a SaaS environment.

40. In section 4.2.2.1, you state that the solution must be able to integrate with Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Ultimate Kronos Group (UKG). Can you elaborate on each service for the expected integrations? *Example: Authentication. For AD does that mean Kerberos and LDAP(s) or both?*

    a. We encourage the vendor to provide all possible solutions for each requirement. Please provide all capabilities of your solution.

41. For question 4.3.1.2, what are you trying to achieve with custom API access controls?

    a. The goal of an RFP is to find the possibilities a vendor can provide. If the vendor has the ability to provide custom API calls, we encourage the vendor to elaborate on those possibilities.

42. For question 4.3.1.8, is there a list of expected Radius protocols needed?

    a. No.

43. For question 4.3.1.15, are there any non-standard-based (SAML, OAuth, OIDC) IdPs under consideration for federation?

    a. No, the reason is that we are planning on changing some of the protocols as part of this project that will not involve any work from the vendor. The vendor must simply be able to propose the standard protocols they provide as part of their solution in the RFP.

44. For question 4.3.1.27, is this about user login, admin login, or both?

    a. Both

45. For question 4.3.1.53, is there a list of compliance requirements to compare against?

    a. This question is a yes/no; however, the vendor can provide a list of currently supported compliance standards.

46. For question 4.3.1.73, can you elaborate on how you want to integrate with Active Roles Server?

    a. This is a yes/no question. We are seeking to know if your system will natively support this service.

47. Would the State consider a 2 weeks extension for vendors to process inputs to questions and submit a meaningful response to the RFP?

    a. Please see answer to question number #6

48. Are you open to extending the submission deadline?

    a. Please see answer to question number #6

49. The RFP indicates integration with "Other applications currently hosted and maintained by the ERP board". How many applications are in scope, and is a list of those applications available?

    a. The service we are requesting should be able to handle multiple applications simultaneously and allow wvOASIS to add and remove applications as needed.

       We are requesting a solution that can add and remove an unlimited number of environments.

50. "The estimated range should be greater than 30,000 users." How many users must the system be able to support?

    a. The actual user logins, both unique and total, are now listed as part of this addendum. Please use these numbers as a basis for performance and pricing.

51. The RFP indicates Budget, Financials and HRM. Are there other departments to consider? What is the approximate number of users for each?

    a. The service we are requesting should be able to handle multiple applications simultaneously and allow wvOASIS to add and remove applications as needed. The actual user logins, both unique and total, are now listed as part of this addendum. Please use these numbers as a basis for performance and pricing. Any user should be able to be provisioned to any application.

52. Is there a target date to have transitioned all users from the current system?

    a. No target dates have been established. This is a SaaS solution and wvOASIS's plan is to move users and applications as necessary to the cloud solution. The transition of users will be conducted by the State.

53. Does the state require bidders to be on-site for the implementation of the solution? Or can the implementation be done remotely?

    a. The pricing sheet requests both onsite assistance and remote assistance.

54. We noticed that the estimated number of hours for the completion of the implementation is listed as 120 hours. Based on our experience and understanding of similar projects, we believe that the estimated hours provided in the pricing template are considerably lower than what is typically required for a successful implementation. Could you please provide further clarification on how these estimates were determined?

    a. The hours and rates are being used for evaluation of the contract and for evaluation purposes only. Please provide your rate based on the pricing sheet.

55. Authentication Management -- B2B / Partner Users: Authorized Users that are third-party consultants, contractors, or vendors of Customer or its Affiliates. How many of the B2B Users? And approximate Users per B2B organization?

    a. The goal of the RFP is to provide an identity manager for both current applications and future applications.

56. Authentication Management -- B2E / Employee / Workforce Users: Authorized Users that are employees of Customer or its Affiliates. How many of the B2E Users?

    a. The goal of the RFP is to provide an identity manager for both current applications and future applications.

57. How many of the B2E Users also require the Analytics Service (Dashboard Toolkit, Anomaly Detection, Event Explorer)?

    a. This would be handled centrally within OASIS. You can estimate 10 users.

58. Authentication Management -- B2C / Customer Users: Customer's customers/consumers who utilize a service offered by Customer or its Affiliates. How many of the B2C Users, if any?

    a. The goal of the RFP is to provide an identity manager for both current applications and future applications.

59. Is consumer identity (CIAM) a component project? What numbers of apps & users are associated with this portion if any?

    b. Please bid accordingly to the capabilities of your solution. Users should be able to access an unlimited number of applications. The user counts have now been provided and is labeled as EXHIBIT B - State of WV Unique Login History

60. Is there a requirement for centralized SSO and MFA solution for cloud and on-prem applications?

    a. This RFP is proposing the moving of a custom SSO/MFA to the cloud. So, the vendor will be the new centralized SSO/MFA for all applications.

61. How many existing users per directory type?

    a. This number would fluctuate between directory types. The service we are requesting should be able to handle multiple applications simultaneously and allow OASIS to add and remove applications as needed.

62. Do you require or integrate any Identity verification services such as license or passport verification?

    a. Please provide your solution's capabilities. As a reminder, these are desirables, not requirements.

63. Does the MFA solution need to enforce conditional access policies across things other than applications such as endpoints, mobile devices and VPNs?

    a. No

64. Is there a need to support a wide range of AuthN factors such as SMS/Biometric/FIDO 2 & QR code-passwordless AuthN? If yes, what?

    a. Yes, please indicate all types of AuthN factors that your solution provides.

65. Does the solution need to provide users with direct access to on-prem and web apps without VPN?

    a. Yes. However, the Solution will integrate into an internet facing system.

66. Does the solution need to provide desktop-delivered MFA for Windows and Mac Machines?

    a. Please indicate all types of MFA that you provide with your solution.

67. Are you looking for OOTB dashboard analytics that can be easily integrated with 3rd party SIEM tools and data repositories?

    a. Please indicate the capabilities of your solution. As a reminder, these are desirables and not requirements.

68. Does the solution need to integrate with third-party SIEM tools for real-time alerting and reporting?

    b. Please indicate the capabilities of your solution. As a reminder, these are desirables and not requirements.

69. Do you currently use an Identity Proofing solution? If yes, what is it?

    a. Not Applicable. Please provide the capabilities of your solution. As a reminder, these are desirables, not requirements.

70. Are there any external Identity Provider (IdP) Federation Services required? Note: this is a user authenticating from outside of the Identity Environment being authenticated by a different IdP that requires access to your applications.

    a. Please provide the capabilities of your solution. As a reminder, these are desirables, not requirements.

71. How many domains will be federated?

    a. Please provide the capabilities of your solution. As a reminder, these are desirables, not requirements.

72. Would you like our solution to Federate your identities in our environment or integrate with another IdP?

    a. No

73. Is this project for a Single Forest / Single Active Directory Domain?

    a. Please provide the capabilities of your solution. As a reminder, these are desirables, not requirements.

74. Please describe any basic or advanced lifecycle management Provisioning required.

    a. None. This is not a request of this RFP.

75. Are your current applications hosted on-site? For example, IIS or Web Portal. (Y/N)

    a. The solution should not be fixed to onsite or hosted. Each application could change over the life of the current contract.

76. Do you currently host any applications in the cloud? (Y/N)

    a. See question #75

77. Will end users be able to update their own profile information (mobile phone, etc.)? (Y/N

    a. Yes.

78. Please list RADIUS supported applications that need MFA as part of this project.

    a. We are not listing applications. This RFP is requesting capabilities of your single sign-on solution.

       We are requesting a solution that can add and remove an unlimited number of applications.

79. Will end users be able to register a new account for themselves (self-service)? (Y/N)

    a. Yes

80. Will end users be able to change their own password (self-service)? (Y/N)

    a. Yes

81. Will there be a need to integrate mobile devices such as iOS and Android? (Y/N)

    a. Yes

82. Will users have the ability to access applications from a mobile device? (Y/N)

    a. Yes

83. Will native deployment of mobile applications be required such as iOS and Android? (Y/N)

    a. No. All mobile devices are general web based system. There is no integration for mobile specific applications.

84. Can you provide more detail about your current Active Directory (AD), LDAP, and Ultimate Kronos Group (UKG) configuration and data structure?

    a. No, vendor should respond based on info given in the RFP.

85. What is the existing identity and access management process in place for the MyApps custom system?

    a. MyApps is a custom in-house application that we are looking to replace with this RFP. This is not relevant to the RFP.

86. How do you prefer to manage user onboarding and offboarding?

    a. Please provide the capabilities of your solution. As a reminder, these are evaluated as desirables and not requirements.

87. Will you want to replace your provisioning (Lifecycle Management) process in this project?

    a. No

88. Can you elaborate on the specific authentication protocols and user data that will need to be migrated from your custom identity system?

    a. This would depend on the solution. OASIS does suggest the vendor provide either examples or opportunities that could be leveraged for user data.

89. Which applications are currently managed by the MyApps system, and what authentication methods do they use?

    a. This is not relevant. Please provide the capabilities of your solution.

       We are requesting a solution that can add and remove an unlimited number of applications.

90. Do you have any specific security policies or risk assessments related to identity and access management that we should be aware of?

    a. No

91. Can you elaborate on the specifics of custom applications and workflows that need to integrate with the identity management solution via API?

    a. No, the proposal should be based on the information given in this RFP.

92. What MFA methods are you currently considering? Which would you prefer implementing first?

    a. The vendor should provide the method(s) that they are proposing for this solution.

93. Are you interested in adaptive authentication features that adjust authentication strength based on risk factors or roles?

    a. Yes, see section 4.3.1.14.

94. Will the State consider modifying Article 26 of the proposed contract terms and conditions to allow a provider's Software License, Data Use, and Support Agreements to take precedence if there is a direct conflict between the contract and the affiliated documents and attachments?

    a. The vendor should assume all legalese will be in place per the RFP.

95. Is the state interested in leveraging a contractor's Federal Supply Schedule(s) for potential advantages?

    a. No, not at this time.

96. Will the State consider waiving the SOC1 Type 2 report requirements for a Systems Integrator (Contractor) if the software provider can satisfy this requirement for the offered solution?

    a. No.

97. In a future phase, will there be a need for Identity Lifecycle Management? For example, automatically creating user accounts for someone who has been hired into the HCM system? Or automatic termination after someone leaves?

    a. The RFP does not cover this activity.

98. Can you please confirm if electronic submission will be acceptable?

a. Electronic Submissions are not allowed for this solicitation.

Please see the following under Instructions to Vendors Submitting Bids section 6 paragraph 3 For Request for Proposal "RFP" Responses Only:

6. BID SUBMISSION: All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through wvOASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through wvOASIS at its sole discretion. Such a prohibition will be contained and communicated in the wvOASIS system resulting in the Vendor's inability to submit bids through wvOASIS. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via email. Bids submitted in paper or facsimile form must contain a signature. Bids submitted in wvOASIS are deemed to be electronically signed.

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

For Request for Proposal ("RFP") Responses Only: Submission of a response to a Request for Proposal is not permitted in wvOASIS. In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal prior to the bid opening date and time identified in Section 7 below, plus _____ convenience copies of each to the Purchasing Division at the address shown below. Additionally, the Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

99. Do you have a Microsoft agreement , if yes please provide the details.

a. Yes, that information is available on the WV Purchasing Division's website at the following link: https://www.state.wv.us/admin/purchase/swc/LAR.htm

100. We are Nasdaq listed fortune 500 company . Please let us know what accounting procedure other than SSAE No. 18 SOC 1 Type 2 is acceptable as asking for just one procedure makes the ask/requirement very narrow and constrained.

a. No, this requirement is met by other corporations that we do business with and is required as part of our single audit for the State.

Revised Specifications

Original specification Section 4.3.1.75. is now deleted.

Specification Section 4.3.1.75. is now revised to state:

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. The vendor must provide the three references upon request but must be provided prior to contract award.

Exhibit B - State of WV Unique Login History

Year-Month	Total Unique Logins
2023-01	24,815
2023-02	23,517
2023-03	23,272
2023-04	23,198
2023-05	22,924
2023-06	23,208
2023-07	23,748
2023-08	23,779
2023-09	23,488
2023-10	23,644
2023-11	23,764
2023-12	23,856

Year-Month	Total Logins
2023-01	302,899
2023-02	266,080
2023-03	301,767
2023-04	274,349
2023-05	299,442
2023-06	291,027
2023-07	289,443
2023-08	314,080
2023-09	282,459
2023-10	302,255
2023-11	285,462
2023-12	264,015

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.

c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.

e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.

f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.

g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.

h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to *store* public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

a) Incident Response: The service provider may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.

b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.

c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at https://apps.wv.gov/ot/ir/Default.aspx, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.

c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.

d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.

b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.

c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

d) The public jurisdiction shall be entitled to any post-termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of the Contract.

e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics.

14. Security:

a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.

c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all personal data.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

a. Access and use the service for its business purposes;
b. For SaaS, use underlying software as embodied or used in the service; and
c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency: _____

Signature: _____

Title: _____

Date: _____

Name of Vendor: Converge Technology Solutions US LLC

Signature: DocuSigned by: Karen Smallwood FD6598FB840A4D2...

Title: Director of Contracts and Compliance

Date: 4/2/24

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: _____

Name of Agency: _____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
   Yes ☐
   No ☐
2. If yes to #1, does the restricted information include personal data?
   Yes ☐
   No ☐
3. If yes to #1, does the restricted information include non-public data?
   Yes ☐
   No ☐
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
   Yes ☐
   No ☐
5. Provide name and email address for the Department privacy officer:

   Name: _____

   Email address: _____

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

   Name: _____

   Email address: _____

   Phone Number: _____ _____

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP ERP24*02

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[ ]	Addendum No. 1	[ ]	Addendum No. 6
[X]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Converge Technology Solutions US LLC

Company

DocuSigned by:
karen Smallwood
FD6598FB840A4D2...

Authorized Signature

4/2/24

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Revised 6/8/2012

Identity Management Single Sign-On Solution RFP with signatures

Following this page, please find the Identity Management Single Sign-On Solution RFP; Central Master Agreement (Proc Type) with signature pages.

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 **Doc Description:** Identity Management Single Sign-On Solution **Proc Type:** Central Master Agreement			**Reason for Modification:**
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: VS0000041625
Vendor Name : Converge Technology Solutions US LLC
Address : 130
Street : Technology Parkway, Suite 100
City : Peachtree Corners
State : GA **Country :** USA **Zip :** 30092
Principal Contact : Charlie Arnett
Vendor Contact Phone: 304-549-7698 **Extension:**

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

Vendor Signature X **FEIN#** 82-2782457 **DATE** 4/2/24

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

ADDITIONAL INFORMATION

The State of West Virginia Purchasing Division, is soliciting bids for the West Virginia Enterprise Resource Planning Board, to establish an open-end contract for a cloud based single sign on solution to manage login profiles, per the attached documentation.

****

ELECTRONIC SUBMISSION IS PROHIBITED FOR THIS RFP

INVOICE TO	SHIP TO
ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US	ENTERPRISE RESOURCE PLANNING BOARD 1007 BULLITT STREET SUITE 400 CHARLESTON WV 25301 US

Line	Comm Ln Desc	Qty	Unit of Measure	Unit Price	Total Price
1	See Exhibit A - Pricing Page				

Comm Code	Manufacturer	Specification	Model #
81112501			

Extended Description:
See attached documentation for complete details.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Vendor Technical Questions due by 2:00PM EST	2024-03-01

REQUEST FOR PROPOSAL
(WV ERP Board and CRFP ERP24*01)

TABLE OF CONTENTS

SECTION 1: GENERAL INFORMATION

1.1. Introduction:

The West Virginia Department of Administration, Purchasing Division (hereinafter referred to as the "Purchasing Division") is issuing this solicitation as a request for proposal ("RFP"), as authorized by W. Va. Code §5A-3-10b, for the WV Enterprise Resource Planning Board (hereinafter referred to as the "Agency") to provide a cloud based single sign on solution to manage login profiles with efficiency and with top-notch security standards. This is a replacement for the current MyApps system used by the State of WV to manage users of Statewide systems.

The RFP is a procurement method in which vendors submit proposals in response to the request for proposal published by the Purchasing Division. It requires an award to the highest scoring vendor, rather than the lowest cost vendor, based upon a technical evaluation of the vendor's technical proposal and a cost evaluation. This is referred to as a best value procurement. Through their proposals, vendors offer a solution to the objectives, problem, or need specified in the RFP, and define how they intend to meet (or exceed) the RFP requirements.

REQUEST FOR PROPOSAL
(WV ERP Board and CRFP ERP24*01)

SECTION 2: INSTRUCTIONS TO VENDORS SUBMITTING BIDS

Instructions begin on next page.

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. REVIEW DOCUMENTS THOROUGHLY: The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

2. MANDATORY TERMS: The Solicitation may contain mandatory provisions identified by the use of the words "must," "will," and "shall." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

3. PREBID MEETING: The item identified below shall apply to this Solicitation.

☑ A pre-bid meeting will not be held prior to bid opening

☐ A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the mandatory pre-bid meeting. Failure to attend the mandatory pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing.

Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

All Vendors should arrive prior to the starting time for the pre-bid. Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

4. VENDOR QUESTION DEADLINE: Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions must be submitted on or before the date listed below and to the address listed below to be considered. A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are nonbinding.

Submitted emails should have the solicitation number in the subject line.

Question Submission Deadline: March 1, 2024 at 2:00PM EST

Submit Questions to: Tara L. Lyle
2019 Washington Street, East
Charleston, WV 25305
Fax: (304) 558-3970
Email: tara.l.lyle@wv.gov

5. VERBAL COMMUNICATION: Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

6. BID SUBMISSION: All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through *wv*OASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through *wv*OASIS at its sole discretion. Such a prohibition will be contained and communicated in the *wv*OASIS system resulting in the Vendor's inability to submit bids through *wv*OASIS. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via email. Bids submitted in paper or facsimile form must contain a signature. Bids submitted in *wv*OASIS are deemed to be electronically signed.

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

For Request for Proposal ("RFP") Responses Only: Submission of a response to a Request for Proposal is not permitted in *wv*OASIS. In the event that Vendor is responding to a request for proposal, the Vendor shall submit one original technical and one original cost proposal prior to the bid opening date and time identified in Section 7 below, plus _____convenience copies of each to the Purchasing Division at the address shown below. Additionally, the Vendor should clearly identify and segregate the cost proposal from the technical proposal in a separately sealed envelope.

Bid Delivery Address and Fax Number:
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Fax: 304-558-3970

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:
BUYER:
SOLICITATION NO.:
BID OPENING DATE:
BID OPENING TIME:
FAX NUMBER:

7. BID OPENING: Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by *wv*OASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery).

Bid Opening Date and Time: March 12, 2024 at 1:30PM EST

Bid Opening Location: Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

8. ADDENDUM ACKNOWLEDGEMENT: Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgment Form, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

9. BID FORMATTING: Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

10. ALTERNATE MODEL OR BRAND: Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand should clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items may be grounds for rejection of a Vendor's bid.

☐ This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

11. EXCEPTIONS AND CLARIFICATIONS: The Solicitation contains the specifications that shall form the basis of a contractual agreement. Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid. Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

12. COMMUNICATION LIMITATIONS: In accordance with West Virginia Code of State Rules §148-1-6.6, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

13. REGISTRATION: Prior to Contract award, the apparent successful Vendor must be properly registered with the West Virginia Purchasing Division and must have paid the $125 fee, if applicable.

14. UNIT PRICE: Unit prices shall prevail in cases of a discrepancy in the Vendor's bid.

15. PREFERENCE: Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

15A. RECIPROCAL PREFERENCE: The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

16. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES: For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37 and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women- owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.

17. WAIVER OF MINOR IRREGULARITIES: The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.6.

18. ELECTRONIC FILE ACCESS RESTRICTIONS: Vendor must ensure that its submission in *wv*OASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

19. NON-RESPONSIBLE: The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1-5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance."

20. ACCEPTANCE/REJECTION: The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.5. and § 148-1-6.4.b."

21. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

22. WITH THE BID REQUIREMENTS: In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.6. This authority does not apply to instances where state law mandates receipt with the bid.

23. EMAIL NOTIFICATION OF AWARD: The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor *wv*OASIS or the Purchasing Division's website to determine when a contract has been awarded.

24. ISRAEL BOYCOTT CERTIFICATION: Vendor's act of submitting a bid in response to this solicitation shall be deemed a certification from bidder to the State that bidder is not currently engaged in, and will not for the duration of the contract, engage in a boycott of Israel. This certification is required by W. Va. Code § 5A-3-63.

REQUEST FOR PROPOSAL
(WV ERP Board and CRFP ERP24*01)

SECTION 3: GENERAL TERMS AND CONDITIONS

Terms and conditions begin on next page.

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

2. DEFINITIONS: As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

2.1. "Agency" or **"Agencies"** means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

2.2. "Bid" or **"Proposal"** means the vendors submitted response to this solicitation.

2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

2.9. "Vendor" or **"Vendors"** means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

3. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☑ **Term Contract**

Initial Contract Term: The Initial Contract Term will be for a period of three (3) years. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

☐ **Alternate Renewal Term** – This contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

☐ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____ days.

☐ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

☐ the contract will continue for _____ years;

☐ the contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

☐ **One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

☐ **Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and continues until the project for which the vendor is providing oversight is complete.

☐ **Other:** Contract Term specified in _____

4. AUTHORITY TO PROCEED: Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

5. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

☐ **Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

☑ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

☐ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

☐ **One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

☐ **Construction:** This Contract is for construction activity more fully defined in the specifications.

6. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

7. REQUIRED DOCUMENTS: All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

☐ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

☐

☐

☐

☐

The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

☑ **Commercial General Liability Insurance** in at least an amount of: $1,000,000.00 per occurrence.

☐ **Automobile Liability Insurance** in at least an amount of: _____ per occurrence.

☐ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: _____ per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

☐ **Commercial Crime and Third Party Fidelity Insurance** in an amount of: _____ per occurrence.

☑ **Cyber Liability Insurance** in an amount of: $5,000,000.00 per occurrence.

☐ **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

☐ **Pollution Insurance** in an amount of: _____ per occurrence.

☐ **Aircraft Liability** in an amount of: _____ per occurrence.

☐

☐

☐

☐

9. WORKERS' COMPENSATION INSURANCE: Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

10. VENUE: All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

11. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

☐ _____ for _____.

☐ Liquidated Damages Contained in the Specifications.

☑ Liquidated Damages Are Not Included in this Contract.

12. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

13. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

14. PAYMENT IN ARREARS: Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

15. PAYMENT METHODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

16. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

18. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

20. TIME: Time is of the essence regarding all matters of time and performance in this Contract.

21. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

22. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

> **SUBCONTRACTOR COMPLIANCE:** Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

23. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

24. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

25. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

26. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

27. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

29. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

30. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in www.state.wv.us/admin/purchase/privacy.

31. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

32. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

33. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

34. VENDOR NON-CONFLICT: Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.

35. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

37. NO DEBT CERTIFICATION: In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

38. CONFLICT OF INTEREST: Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

39. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

☑ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

☐ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.division@wv.gov.

40. BACKGROUND CHECK: In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.

b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open heath, basic oxygen, electric furnace, Bessemer or other steel making process.

c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

    1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars ($2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or

    2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars ($50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a "substantial labor surplus area", as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least $1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

44. PROHIBITION AGAINST USED OR REFURBISHED: Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

45. VOID CONTRACT CLAUSES: This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

46. ISRAEL BOYCOTT: Bidder understands and agrees that, pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

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) Charlie Arnett

(Address) 130 Technology Parkway, Suite 100; Peachtree Corners, GA 30092

(Phone Number) / (Fax Number) 304.549.7698 / 304 768-1645

(email address) Charlie.Arnett@convergetp.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, 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.

Converge Technology Solutions US LLC
(Company)

DocuSigned by:
Karen Smallwood
(Signature of Authorized Representative)

Karen Smallwood, Director Contracts And Contract
(Printed Name and Title of Authorized Representative) (Date)

Karen Smallwood Director of Contracts 4/2/2024 ract Governance
(Phone Number) (Fax Number)

ksmallwood@convergetp.com
(Email Address)

REQUEST FOR PROPOSAL
(WV ERP Board and CRFP ERP24*01)

SECTION 4: PROJECT SPECIFICATIONS

4.1. Background and Current Operating Environment:
Currently the State of WV uses MyApps custom identity management system. This system was developed by the Auditor's office in 2008. This system was also used to manage user access when the WVOASIS system went live in 2013 for Budget, 2014 for Financials and starting in 2015 for the HRM, time and leave system.

There is now a need to standardize on a new platform that will allow the State to manage login profiles with greater efficiency and with greater security standards. The Enterprise Resource Planning Board is issuing this RFP to find a cloud based comprehensive single sign on solution for the use of many third-party applications to include CGI Advantage, UKG, Deighton, and other applications currently hosted and maintained by the ERP Board.

4.2. Project Goals and Mandatory Requirements: In the past three years the OASIS system has been requested to provide multiple forms of data to the critical agency system to include some of those listed above. This helps in the reduction of duplication of data, duplication of user entry of this data and to provide a central source for data. As this expands in the future, there needs to be a secure mechanism for user interaction. That user interaction we believe will come from a new cloud-based identity management system. Vendor should describe its approach and methodology to providing the service or solving the problem described by meeting the goals/objectives identified below. Vendor's response should include any information about how the proposed approach is superior or inferior to other possible approaches.

4.2.1. Goals and Objectives – The project goals and objectives are listed below.

4.2.1.1 Provide a state-wide solution for the ERP solution and supporting applications to provide a single sign on solution.

4.2.1.2 Obtain a complete single sign solution that is cloud based and will provide robust security solutions to include encryption, logging, and provide common industry standard options for a single sign on solution.

4.2.2. Mandatory Project Requirements – The following mandatory requirements relate to the goals and objectives and must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it will comply with the mandatory requirements and include any areas where its proposed solution exceeds the mandatory requirement. Failure to comply with mandatory requirements will lead to disqualification, but the approach/methodology that the vendor uses to comply, and areas where the mandatory requirements are exceeded, will be included in technical scores where appropriate. The mandatory project requirements are listed below.

4.2.2.1 The solution must be able integrate with our existing identity sources including Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Ultimate Kronos Group (UKG)

4.2.2.2 The solution must provide a seamless migration path for users from our existing identity infrastructure.

4.2.2.3 Authentication methods must include SAML2.0, SP(Service Provider) and IDP (Identity Provider) methods of authentication.

4.2.2.4 The solution presented must be cloud-based.

4.3. Qualifications and Experience: Vendor should provide information and documentation regarding its qualifications and experience in providing services or solving problems similar to those requested in this RFP. Information and documentation should include, but is not limited to, copies of any staff certifications or degrees applicable to this project, proposed staffing plans, descriptions of past projects completed (descriptions should include the location of the project, project manager name and contact information, type of project, and what the project goals and objectives where and how they were met.), references for prior projects, and any other information that vendor deems relevant to the items identified as desirable or mandatory below.

Qualification and Experience Information: Vendor should describe in its proposal how it meets the desirable qualification and experience requirements listed below.

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.

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.

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.

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

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

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

4.3.1.7. Detail the scalability of your Application Programming Interface infrastructure to support high volumes of authentication and authorization requests.

4.3.1.8. Does your solution provide Remote Authentication Dial-In User Service (RADIUS) support that does not require on-premise components?

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.

4.3.1.10. List the Multi-factor methods supported.

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

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.

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.

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

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

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.

4.3.1.17. Explain how your solution adapts authentication methods based on contextual factors like location and device.

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

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

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

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

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

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

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

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?

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

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

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

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

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

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?

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

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?

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.

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

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.

4.3.1.36. Do you have an administrator dashboard User Interface (UI) to manage users? Can you enforce a specific multi-factor type for administrative access?

4.3.1.37. Does the solution support external federation? If so, how, and what Identity Providers (IdPs) are supported?

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

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

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

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? (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?

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

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

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

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?

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.

4.3.1.48. How long are the logs maintained?

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

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

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

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

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

4.3.1.54. What options are available for exporting logs and reports to external systems or Security information and event management (SIEM) solutions?

4.3.1.55. Indicate and identify any countries where you provide services to clients outside of the United States (and US territories).

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.

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

4.3.1.58. Where does the solution reside?

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.

4.3.1.60. Describe how your service provides failover and redundancy.

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

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

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

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

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

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

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

4.3.1.68. Are sessions cleared upon logging off?

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

4.3.1.70. Describe your approach to managing long-running sessions

4.3.1.71. How does your platform manage user sessions in scenarios where users access applications from various locations?

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

4.3.1.73. Does your solution integrate with Active Roles Server?

4.3.1.74. Explain how your platform complies with industry standards and regulations related to data security and privacy.

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.

4.4.Mandatory Qualification/Experience Requirements – The following mandatory qualification/experience requirements must be met by the Vendor as a part of its submitted proposal. Vendor should describe how it meets the mandatory requirements and include any areas where it exceeds the mandatory requirements. Failure to comply with mandatory requirements will lead to disqualification, but areas where the mandatory requirements are exceeded will be included in technical scores where appropriate. The mandatory qualifications/experience requirements are listed below.

4.4.1.1. Vendor must provide SSAE No. 18 SOC 1 Type 2 report results yearly to satisfy overall State of WV SOC1 requirements.

SECTION 5: VENDOR PROPOSAL

5.1. Economy of Preparation: Proposals should be prepared simply and economically providing a concise description of the items requested in Section 4. Emphasis should be placed on completeness and clarity of the content.

5.2. Incurring Cost: Neither the State nor any of its employees or officers shall be held liable for any expenses incurred by any Vendor responding to this RFP, including but not limited to preparation, delivery, or travel.

5.3. Proposal Format: Vendors should provide responses in the format listed below:

5.3.1. Two-Part Submission: Vendors must submit proposals in two distinct parts: technical and cost. Technical proposals must not contain any cost information relating to the project. Cost proposal must contain all cost information and must be sealed in a separate envelope from the technical proposal to facilitate a secondary cost proposal opening.

5.3.2. Title Page: State the RFP subject, number, Vendor's name, business address, telephone number, fax number, name of contact person, e-mail address, and Vendor signature and date.

5.3.3. Table of Contents: Clearly identify the material by section and page number.

5.3.4. Response Reference: Vendor's response should clearly reference how the information provided applies to the RFP request. For example, listing the RFP number and restating the RFP request as a header in the proposal would be considered a clear reference.

Proposal Submission: All proposals (both technical and cost) must be submitted to the Purchasing Division **prior** to the date and time listed in Section 2, Instructions to Vendors Submitting Bids as the bid opening date and time.

SECTION 6: EVALUATION AND AWARD

6.1. Evaluation Process: Proposals will be evaluated in two parts by a committee of three (3) or more individuals. The first evaluation will be of the technical proposal and the second is an evaluation of the cost proposal. The Vendor who demonstrates that it meets all of the mandatory specifications required, attains the minimum acceptable score and attains the highest overall point score of all Vendors shall be awarded the contract.

6.2. Evaluation Criteria: Proposals will be evaluated based on criteria set forth in the solicitation and information contained in the proposals submitted in response to the solicitation. The technical evaluation will be based upon the point allocations designated below for a total of 70 of the 100 points. Cost represents 30 of the 100 total points.

Evaluation Point Allocation:

The evaluation questions in Section 4.3 have been divided into three levels (High, Medium, and Low).

High Requirement Level (42 responses):	15 Points Maximum (each)
Medium Requirement Level (24 responses):	10 Points Maximum (each)
Low Requirement Level (8 responses):	5 Points Maximum (each)

A total of 910 points can be earned from responses to these evaluation questions.

Total Technical Score:	910 Points Possible
Total Cost Score:	390 Points Possible

Total Proposal Score: 1300 Points Possible

6.3. Technical Bid Opening: At the technical bid opening, the Purchasing Division will open and announce the technical proposals received prior to the bid opening deadline. Once opened, the technical proposals will be provided to the Agency evaluation committee for technical evaluation.

6.4. Technical Evaluation: The Agency evaluation committee will review the technical proposals, assign points where appropriate, and make a final written recommendation to the Purchasing Division.

6.5. Proposal Disqualification:

6.5.1. **Minimum Acceptable Score ("MAS"):** Vendors must score a minimum of 70% (49 points) of the total technical points possible in order to move past the technical evaluation and have their cost proposal evaluated. All vendor proposals not attaining the MAS will be disqualified.

6.5.2. **Failure to Meet Mandatory Requirement:** Vendors must meet or exceed all mandatory requirements in order to move past the technical evaluation and have their cost proposals evaluated. Proposals failing to meet one or more mandatory requirements of the RFP will be disqualified.

6.6. Cost Bid Opening: The Purchasing Division will schedule a date and time to publicly open and announce cost proposals after technical evaluation has been completed and the Purchasing Division has approved the technical recommendation of the evaluation committee. All cost bids received will be opened. Cost bids for disqualified proposals will be opened for record keeping purposes only and will not be evaluated or considered. Once opened, the cost proposals will be provided to the Agency evaluation committee for cost evaluation.

The Purchasing Division reserves the right to disqualify a proposal based upon deficiencies in the technical proposal even after the cost evaluation.

We are requesting an initial contract term of three years, with the option to renew for three additional one-year periods. Please complete the pricing page for all six years.

6.7. Cost Evaluation: The Agency evaluation committee will review the cost proposals, assign points in accordance with the cost evaluation formula contained herein and make a final recommendation to the Purchasing Division.

Cost Evaluation Formula: Each cost proposal will have points assigned using the following formula for all Vendors not disqualified during the technical evaluation. The lowest cost of all proposals is divided by the cost of the proposal being evaluated to generate a cost score percentage. That percentage is then multiplied by the points attributable to the cost proposal to determine the number of points allocated to the cost proposal being evaluated.

Step 1: Lowest Cost of All Proposals / Cost of Proposal Being Evaluated = Cost Score Percentage

Step 2: Cost Score Percentage X Points Allocated to Cost Proposal = **Total Cost Score**

Example:

Proposal 1 Cost is $1,000,000
Proposal 2 Cost is $1,100,000

Points Allocated to Cost Proposal is 30

Proposal 1: Step 1 – $1,000,000 / $1,000,000 = Cost Score Percentage of 1 (100%)
Step 2 – 1 X 30 = Total Cost Score of 30

Proposal 2: Step 1– $1,000,000 / $1,100,000 = Cost Score Percentage of 0.909091 (90.9091%)
Step 2 – 0.909091 X 30 = Total Cost Score of 27.27273

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Converge Technology Solutions US LLC

(Company)

Karen Smallwood, Director of Contract and Compliance

(Representative Name, Title)

866.910.4425

(Contact Phone/Fax Number)

4/2/24

(Date)