

TECHNICAL PROPOSAL

IDENTITY MANAGEMENT SINGLE SIGN-ON SOLUTION

REQUEST FOR PROPOSALS NO. CRFP 0947 ERP2400000002



State of West Virginia

Submitted to:

Larry D McDonnell
State of West Virginia
Department of Administration,
Purchasing Division 2019 Washington Street E:
Charleston, WV 25305-0130
Phone: 304-558-3970

Opening Date: February 23rd, 2024

Deadline for Questions: March 1st, 2024

Technical Proposal Due Date: April 4th, 2024

Financial Proposal Due Date: April 4th, 2024

ORIGINAL



Submitted by:

Software Productivity Strategists, Inc.

2400 Research Blvd. Suite 115
Rockville, MD 20850
301-337-2290

Mary Stang | Director – State, Local Education

Email: mary.stang@spsnet.com

Signature:

A handwritten signature in black ink that reads "Mary Stang".

RECEIVED

2024 APR -4 AM 9: 15

WV PURCHASING
DIVISION



Table of Contents

COVER LETTER	3
EXECUTIVE MANAGEMENT SUMMARY	4
4.2 PROJECT GOALS AND MANDATORY REQUIREMENTS:.....	6
4.2.1. GOALS AND OBJECTIVES.....	6
AS IS ARCHITECTURE.....	7
TO BE ARCHITECTURE – PRODUCTION ENVIRONMENT.....	8
INTRODUCTION TO SCOPE OF WORK (SOW).....	9
4.3 QUALIFICATIONS AND EXPERIENCE:.....	17
4.4. MANDATORY QUALIFICATION/EXPERIENCE REQUIREMENTS	51
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.....	51
REFERENCES:.....	52
IDENTITY MANAGEMENT SINGLE SIGN-ON TRAINING PROGRAM.....	53
TEAM RESUMES	55
CRFP ERP24-02 DESIGNATED CONTACT	110
CRFP ERP24-02 AVAILABILITY OF INFORMATION.....	111
CRFP 0947 ERP2400000002 2 WV CRFP FORM	112
CRFP ERP24-02 - ADDENDUM 01.....	115
CRFP ERP24-02 - ADDENDUM 02.....	120

COVER LETTER

Larry D McDonnell
West Virginia Oasis
Department of Administration Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Email ID: larry.d.mcdonnell@wv.gov

March 16, 2024

Dear Larry,
Software Productivity Strategists, Inc. is pleased to submit the following proposal:

RFP: CRFP 0947 ERP2400000002
Bid Title: IDENTITY MANAGEMENT SINGLE SIGN-ON SOLUTION

We acknowledge the receipt of the following:

Opening Date: February 23rd, 2024
Pre-Proposal Conference: N/A
Deadline for Questions: March 1st, 2024
Technical Proposal Due Date: March 26th, 2024
Financial Proposal Due Date: March 26th, 2024
Addendum 1 – dated March 6th, 2024
Addendum 2 – dated March 20th, 2024

The requested company details are given below:

Name of Firm: Software Productivity Strategists, Inc.
Main Office Address: 2400 Research Blvd. Suite 115, Rockville, MD 20850
State of Incorporation: Maryland
Incorporated: July 30, 1991
FEIN Number: 52-1832154

If you have any questions concerning this proposal, please contact Mary Stang by phone 301-337-2290 or via email mary.stang@spsnet.com.

Sincerely,



Software Productivity Strategists, Inc.
Mary Stang, Director – State, Local Education

Executive Management Summary

Executive Summary

Software Productivity Strategists, Inc. (SPS), with over 25 years of Identity and Access Management (IAM) expertise, is proud to propose IBM Security Verify as the solution to the West Virginia Enterprise Resource Planning Board's Request for Proposal (RFP) for a cloud-based Identity Management Single Sign-On Solution. Our long-standing history in delivering IAM solutions positions us uniquely to meet the State's need for a system that enhances operational efficiency and security standards. This executive summary elaborates how IBM Security Verify seamlessly aligns with the West Virginia Department of Administration's needs and why SPS, Inc. stands as the ideal partner for this transformative project.

Solution Overview: IBM Security Verify

Leveraging IBM Security Verify, SPS offers a cloud-based identity and access management solution that integrates seamlessly with existing systems, provides robust security measures, and enhances user experience. IBM Security Verify is a modern, cloud-based IAM solution that provides extensive capabilities for identity governance, access management, and multi-factor authentication. It is engineered to support the dynamic and complex requirements of today's digital environment, offering unparalleled security and user convenience. This proposal is in direct response to the RFP's objectives to replace the current MyApps system with a more efficient and secure platform.

Key Solution Features:

- **Seamless Integration:** IBM Security Verify integrates effortlessly with existing identity sources such as Active Directory (AD), LDAP, and Ultimate Kronos Group (UKG), ensuring a smooth transition from the current system and minimizing disruption to user workflows.
- **Robust Security:** The solution incorporates advanced encryption, detailed logging, and supports SAML2.0 for both SP and IDP, enhancing the security posture of the state's digital ecosystem. IBM Security Verify's comprehensive security framework ensures that sensitive information remains protected against emerging threats.
- **User-Centric Design:** By providing single sign-on capabilities, IBM Security Verify simplifies access to multiple applications with a single set of credentials, improving the overall user experience for state employees and reducing the likelihood of password fatigue.
- **Cloud-Based Flexibility:** As a cloud-based solution, IBM Security Verify offers scalability, reliability, and easy access, meeting the RFP's requirement for a cloud-based platform. This architecture ensures that the solution can adapt to the evolving needs of the state without requiring significant infrastructural investments.

SPS Inc. Expertise and Compliance:

- **Extensive IAM Experience:** SPS's quarter-century of expertise in IAM is evidenced by our deep understanding of identity management challenges and our ability to deliver tailored solutions.
- **Annual Compliance Reports:** We commit to providing SSAE No. 18 SOC 1 Type 2 reports annually, demonstrating our dedication to high operational and security standards.
- **Proven Track Record:** Included in our proposal are references from clients with extensive user bases, showcasing our capability to manage large-scale identity management projects successfully.

Software Productivity Strategists, Inc. is enthusiastic about the opportunity to collaborate with the West Virginia Enterprise Resource Planning Board. By proposing IBM Security Verify, we are confident in our ability to significantly

enhance the State's digital infrastructure, providing a secure, efficient, and user-centric single sign-on solution. Our vast experience in IAM ensures that we are well-equipped to execute this project successfully, furthering our commitment to advancing the State's technological capabilities.

Sincerely,

A handwritten signature in cursive script that reads "Mary Stang".

Software Productivity Strategists, Inc.
Mary Stang, Director – State, Local Education

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

State-wide Solution for ERP and Supporting Applications:

Leveraging IBM Security Verify, we propose a unified and scalable solution that seamlessly integrates with state-wide ERP systems and supporting applications. This approach not only centralizes identity management but also ensures consistent application of security policies across all platforms.

Complete Single Sign-On Solution that is Cloud-Based:

IBM Security Verify, with its cloud-native architecture, offers a comprehensive single sign-on (SSO) experience that simplifies user access while maintaining high security standards. Our cloud-based solution ensures that users can securely access necessary applications from anywhere, at any time, with minimal latency.

Robust Security Solutions:

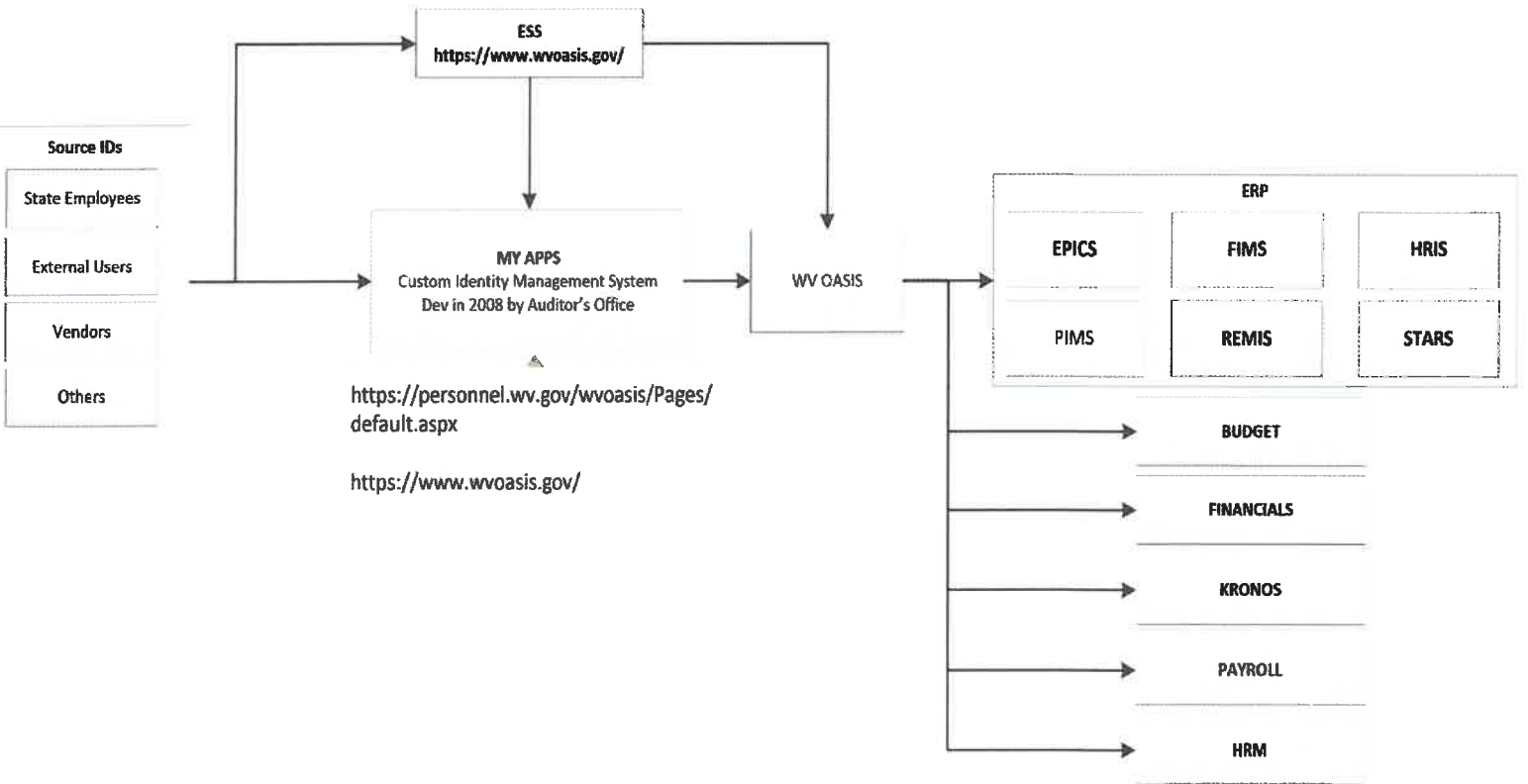
Security is at the forefront of IBM Security Verify. It includes features such as adaptive authentication, risk-based access controls, and end-to-end encryption to safeguard against evolving threats. Our solution ensures compliance with regulatory standards and offers a secure environment for all users.

Common Industry Standard Options for Single Sign-On Solution:

IBM Security Verify supports all major SSO standards, including SAML2.0, OpenID Connect, and OAuth2.0, ensuring compatibility with a wide range of applications and services. Our solution facilitates smooth integration with third-party applications and legacy systems without compromising on security or user experience.

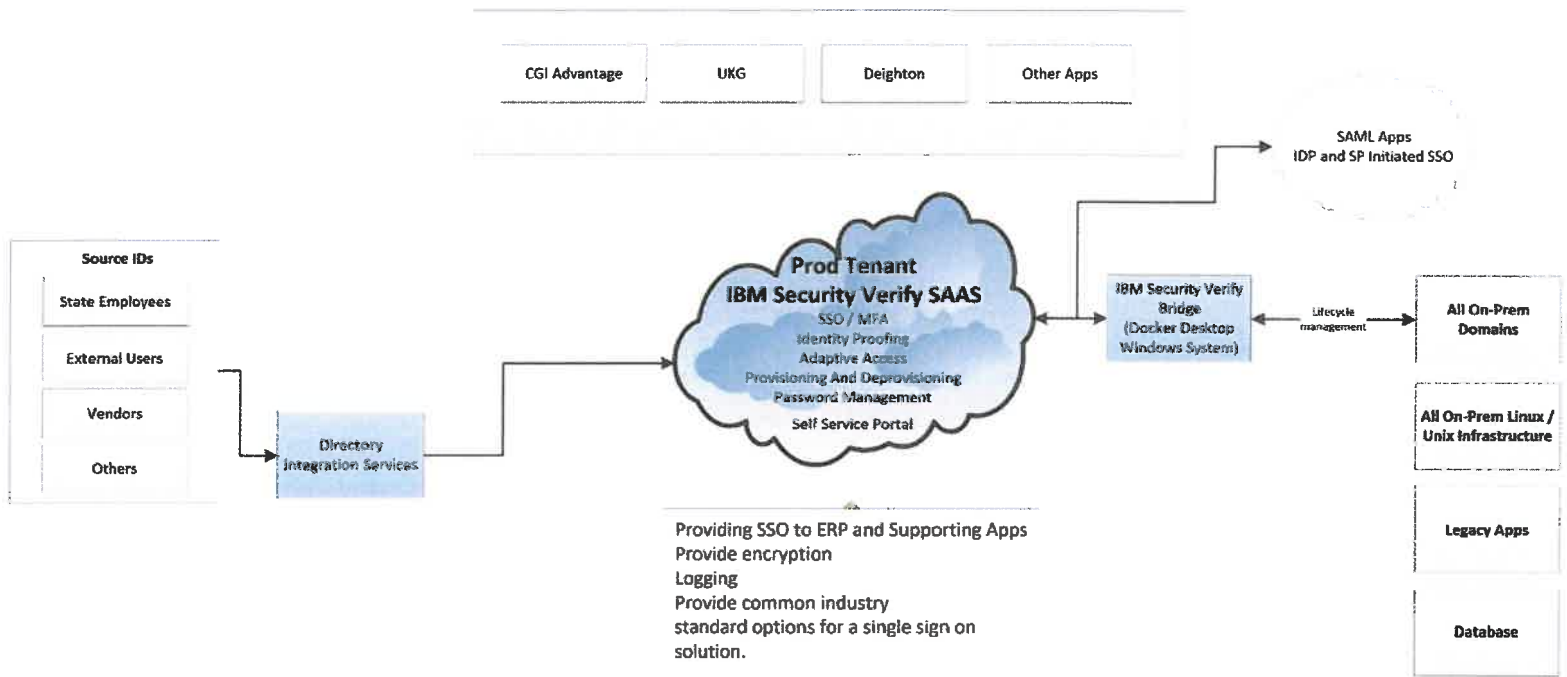
AS IS Architecture

The architecture outlined below is a result of careful analysis and consideration, leveraging our best assumptions about the current systems and future needs of the West Virginia Department of Administration.



TO BE Architecture – Production Environment

The architecture outlined below is a result of careful analysis and consideration, leveraging our best assumptions about the current systems and future needs of the West Virginia Department of Administration.



Introduction to Scope of Work (SOW)

Purpose:

This document serves as the accompanying Scope of Work (SOW) for the proposed Identity Management Single Sign-On Solution at the State of West Virginia. In an effort to provide comprehensive and detailed information about the project deliverables, timelines, and responsibilities, we have included a structured spreadsheet to augment the narrative of this SOW.

No.	Tasks & Activities	SPS Deliverables
	Project Launch (Project Management)	Project Plan Project Portal
	Kick-off Meeting (Procurement, IAM Executive, IAM Manager/PM)	
	Introduction	
	Project portal intro	
	SPS Org chart walkthrough	
	Get Org chart and project team	1. URL of the project portal 2. Request credentials for all participants
	Present Project plan - SOW	
	Implementation schedule including dates/times for key milestones - Installation, Training, Discovery	ProjectPlan.xls
	Present Project plan - SOW	
	Meet the following Stakeholders to schedule dates/times for: Training, Architecture, Deployment, Success Criteria and Project Plan	
	GRC	
	C-level for Governance	
	Risk Officer for Risk	
	Compliance Officer for Compliance	
	Security	
	Executive	
	Tactical	
	Operations	
	IT	
	Executive	
	Tactical	
	Operations	

	Deployment Team	
	IT Staff - Infrastructure	
	IT Staff - Others	
	Requirements Gathering & Discovery	Acceptance Test Document Deployment Document for SAAS
	Site Validation - (IAM Implementer required)	
	Deployment document walkthrough	
	Obtain list of Identity feed attributes from HR feed	ID Feed
	Walk-through of the Active Directory environment to create Acceptance Test use-case. - (Active Directory stakeholder required)	
	Capture AS IS Use-Cases - ITIL IAM FW	
	IAM Manager : Oversees the Access and Integrations teams and projects	
	Roles and KPIs	
	ITIL IAM Framework	
	IAM Runbooks	
	Evaluate and Verify Identity and Access Request	
	Create and Maintain Identity	
	Provide and Maintain Access Rights	
	Monitor Identity and Access	
	Training Program	
	Learning Portal Walkthrough	
	IAM Enterprise Architect – Manager: Over sees the Systems and Integrations team	
	Roles and KPIs	
	ITIL IAM Framework	
	IAM Runbooks	
	Evaluate and Verify Identity and Access Request	
	Create and Maintain Identity	
	Provide and Maintain Access Rights	
	Monitor Identity and Access	
	Training Program	
	Learning Portal Walkthrough	
	IAM Administrator:	
	Roles and KPIs	
	ITIL IAM Framework	
	IAM Runbooks	
	Evaluate and Verify Identity and Access Request	
	Create and Maintain Identity	
	Provide and Maintain Access Rights	
	Monitor Identity and Access	

Training Program	
Learning Portal Walkthrough	
IAM Developer:	
Roles and KPIs	
ITIL IAM Framework	
IAM Runbooks	
Evaluate and Verify Identity and Access Request	
Create and Maintain Identity	
Provide and Maintain Access Rights	
Monitor Identity and Access	
Training Program	
Learning Portal Walkthrough	
IAM Business Analyst:	
Roles and KPIs	
ITIL IAM Framework	
IAM Runbooks	
Evaluate and Verify Identity and Access Request	
Create and Maintain Identity	
Provide and Maintain Access Rights	
Monitor Identity and Access	
Training Program	
Learning Portal Walkthrough	
Create Acceptance test document & obtain signoff	Acceptance Test Document
Identify existing SAAS roles	
Walk-through of self-service password management use-case. Create Acceptance Test use-case. (IAM Manager, IAM Process Owner required)	Self Service Guide
Schedule walk-through of out-of-the-box self-care application	
Get Challenge/Response for Forgotten passwords	
Skill-Gap Analysis of West Virginia Department of Administration's IAM implementation and system administration team to assess readiness for production support. Devise a training program to address those needs. Create Acceptance tests use-cases. (IAM Manager, IAM Process Owner required)	
Architecture and Design	Compose design document
Create System Architecture	
Production Environment	Production.pdf
Validate Production Architecture with IBM	
Deployment	Deployment Documents
Request IBM Security Verify tenants to initiate Deployment	
Setup Production Environment	

	Validate software and networking for Dev environment	
	Installing all IBM modules on West Virginia Department of Administration's infrastructure non-Production environments.	
	Install / Configure the following IAM components using the deployment document:	
	IBM Directory Integrator / Adapter Server	
	Install IBM Directory Integrator	
	Install IBM RMI Dispatcher	
	Install SAAS Adapter Installer	
	IBM Bridge Server	
	Install Docker Desktop	
	Install and Configure Linux Containers	
	Install IBM SAAS tenant Identity Brokerage	
	Configure IBM Security Verify SaaS	Deployment Document for Prod Env
	Configure Realm	
	Integrate on-prem SAAS	
	Configure Access Control Items	
	Configure Multi-Factor Authentication	
	Configure Partners	
	Configure Self-Service	
	Integrate Production Environment	
1	Identity Hub / Registry Implementation	
	Setting up identity feeds from Feed systems (State Employees, External Users, Vendors, and Others)	Data feed Signoff
	The identity feed must include all users groups and simple attributes that will be drawn from one source.	
	Configure SAAS platform to identify, ingest data, and act on that data in near real-time from Workday and other applicable sources and propagate updates to downstream services	
	Establish data cleanup/hygiene and transformations rules	
	Configure hard, soft, and fuzzy matching rules	
	Configure match resolution queue routing and actions	
	Perform full import into the identity hub /registry	
	Create custom person class in SAAS	
	Map Identify source attributes to the SAAS person class	
	Identify attributes to managers, admins, vendors and other groups	
	Define Input Datamap and develop scripts for input maps	

	Define output datamap and perform output attributes mapping	
	Configure and assign unique identifiers	
	Release schema and integration points	
	Configure near real-time dataflow and triggers	
	Define and configure SDI Services	
	Define reconciliation parameters, add scripts for custom attributes and create schedules	
	Test and troubleshoot TDI identity feed service	
	Retire current LDAP update process	
2	State Employees and Affiliate/Guest provisioning, deprovisioning, and birthright entitlements for in-scope SoA and target systems	
	Providing integration with Active Directory.	AD signoff
	Capture current provisioning use-cases	
	Install & configure Active Directory adapter	
	Import AD profile in SAAS and create a service	
	Define Identity, Password and Provisioning policies	
	Configure AD provisioning workflows and parameters	
	Test provisioning and de-provisioning on AD using Automatic and Manual provisioning policies	
	Providing integration with CGI Advantage	CGI Advantage signoff
	Capture current provisioning use-cases	
	Import adapter profile in SAAS and create a service	
	Define Identity, Password and Provisioning policies	
	Configure provisioning workflows and parameters	
	Test provisioning and de-provisioning on target system using Automatic and Manual provisioning policies	
	Providing integration with UKG	UKG signoff
	Capture current provisioning use-cases	
	Install & configure adapter Office 365	
	Import adapter profile in SAAS and create a service	
	Define Identity, Password and Provisioning policies	
	Configure provisioning workflows and parameters	
	Test provisioning and de-provisioning on target system using Automatic and Manual provisioning policies	
	Providing integration Deighton	Deighton signoff
	Capture current provisioning use-cases	
	Configure Identity Provider and Service Providers and setup MFA	
	Define Identity, Password and Provisioning policies	
	Configure provisioning workflows and parameters	
	Test provisioning and de-provisioning on target system using Automatic and Manual provisioning policies	

	Providing integration with SAML based Apps	SAML Apps signoff
	Capture current provisioning use-cases	
	Configure Identity Provider and Service Providers and setup MFA	
	Import adapter profile in SAAS and create a service	
	Define Identity, Password and Provisioning policies	
	Test Adapter, provisioning and Deprovisioning use cases	
	Configure provisioning workflows and parameters	
	Create and install the CERT on ISAM to be used by Federation	
	Creating SSO Configurations	
	Create Federation for IDP	
	Create custom mapping file and attach to the Federation	
	Exchange metadata between ISAM and IDP	
	Import Metadata and add partner	
	Testing for IDP initiated SSO using SAML trace	
	Testing for SP initiated SSO using SAML trace	
	Providing integration with Linux / Windows servers	Linux / Windows servers systems signoff
	Install & configure adapter for SAAS	
	Import adapter profile in SAAS and create a service	
	Define Identity, Password and Provisioning policies	
	Configure provisioning workflows and parameters	
	Test provisioning and de-provisioning on target system using Automatic and Manual provisioning policies	
	Providing integration with Database	Database signoff
	Install & configure adapter for SAAS	
	Import adapter profile in SAAS and create a service	
	Define Identity, Password and Provisioning policies	
	Configure provisioning workflows and parameters	
	Test provisioning and de-provisioning on target system using Automatic and Manual provisioning policies	
	Configure Self Service Portal	
	Password Sync Configurations	
	Testing and troubleshooting	
	Activate/Deactivate self-care features	
3	Sponsored Affiliate/Guest Lifecycle Management	
	Utilize the SAAS platform’s sponsored guest solution to replace all account processes.	
	i. Configure rules, forms, workflows, and approvals.	
	ii. Configure baseline roles and birthright entitlements.	
	iii. Configure the renewal process and notifications.	
	iv. Configure the deprovisioning process.	
4	Account Claim, Password Management, and Identity Administration	
	Utilize the SAAS platform’s sponsored guest solution to replace all account processes.	

	Configure SAAS platform with account claim rules.	
	Configure SAAS platform with account recovery options	
5	Group Entitlement and Access Management	
	a. Configure the solution to automatically create and manage group membership to reflect the organizational structure of West Virginia Department of Administration.	
	b. Configure delegated groups and workflows with approvals.	
	c. Configure mechanism for viewing/managing entitlement requests and approval processes.	
	d. Configure SAAS platform to manage groups and memberships on AD, LDAP, and Google Apps	
	e. Configure rules for institutional affiliation-based groups (e.g., staff, faculty, State Employees, courtesy, family, etc.).	
	f. Configure rules and workflows for delegated groups and group membership.	
	g. Configure the solution and migrate manually managed groups to the new solution.	
	Required MFA	
	a. Implement/integrate MFA services in new SAAS platform	
	Application Authorization and API Services Integration	
	a. Create an inventory of applications that utilize internal authorization	
	b. For each application:	
	i. Analyze roles and map application rights to SAAS entitlements	
	ii. Configure application integration with SAAS (entitlement, group, attribute, database, file, API, etc.)	
	iii. Configure authorization mapping and automation	
	iv. Link roles with fulfillment actions	
	c. Configure API services and determine access rights and service accounts	
	Account & Access Management Workflows & Approvals	
	a. Analyze access needs that exceed automation capabilities	
	b. Translate access needs into entitlements	
	c. Implement delegation for administration of each entitlement	
	d. Implement workflows to ensure requests are routed properly	
	e. Implement approvals for data stewards and/or supervisors	
	f. Implement appropriate group/attribute management workflows	
	g. Configure fulfillment process for each entitlement	
	h. Configure certification/attestation for regulatory compliance	
	i. Configure access certification process and campaigns	
	j. Configure Separation of Duties Policies for access requests	
	IAM Reporting, Monitoring, Certification, and Attestation	
	a. Configure audit policy, reporting, and monitoring	
	b. Configure certification/attestation for regulatory compliance	

	c. Configure access certification process and campaigns	
	d. Configure Separation of Duties Policies for access requests	
	Passwordless Authentication	
	a. Explore options for the implementation of passwordless authentication	
	b. Consider options including public key, token based, and biometric features	
	Communication and go-live planning	
	Set production as LIVE	
	Verify Backup/restores	
	Verify Rollback plan	
	Schedule Go Live	Go Live signoff
	Go-live assistance and post go-live support	
	System Support	
	Provide L2 and L3 resources to assist.	
	System health check activity to be performed once in a quarter	
	Upgrades and fixes as per UA's upgrade SOPs	
	Performance and tuning activity	
	Proactive Monitoring	
	Work with principle OEM for any escalations if needed	
	End User Support	
	Provision of Helpdesk L1 during business hours and workdays	
	Provision of L2 and L3 engineers when the escalation is made from Helpdesk	
	Perform root cause analysis	
	User enablement and support	
	Compose as-built documentation upon conclusion	
	Low Level Design Document	
	High Level Design Document	
	Other documentation sources	

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 were 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.

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

Technical Requirements	
Item	Description
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, applications can integrate directly with IBM Security Verify's Application Programming Interface (API) to perform RESTful API calls for a variety of purposes, including reading user information, making changes to user objects, and managing group membership. IBM Security Verify offers a comprehensive set of APIs that allow for extensive interaction with the solution, enabling automation, customization, and integration with third-party systems or applications.	
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.
<p>IBM Security Verify enables the creation of custom API access policies that govern how APIs can be accessed and used, ensuring that API interactions comply with organizational security policies and regulations. Here are the details regarding custom API access policies and authorization of servers in IBM Security Verify:</p> <ul style="list-style-type: none"> • Custom API Access Policies: Administrators can define custom API access policies within IBM Security Verify. These policies can specify which users or applications are allowed to access certain APIs, under what conditions, and with what permissions. 	

- **Authorized Servers:** IBM Security Verify allows for the specification of authorized servers that can make API calls. This is typically done by registering the server's IP address or by using API keys that are assigned to specific servers or applications.
- **OAuth 2.0 and OpenID Connect Support:** IBM Security Verify supports OAuth 2.0 and OpenID Connect (OIDC) for securing API access.
- **Throttling and Rate Limiting:** To prevent abuse and ensure fair usage, IBM Security Verify supports throttling and rate limiting on its APIs. Administrators can configure these settings as part of the API access policies to control the number of requests that an authorized server can make within a certain timeframe.
- **Logging and Monitoring:** IBM Security Verify provides comprehensive logging and monitoring capabilities for API usage. This enables administrators to audit access, track API calls, and monitor for any unusual or unauthorized activity.

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, IBM Security Verify offers Application Programming Interface (API) token management and creation capabilities. Here are the details regarding these capabilities:

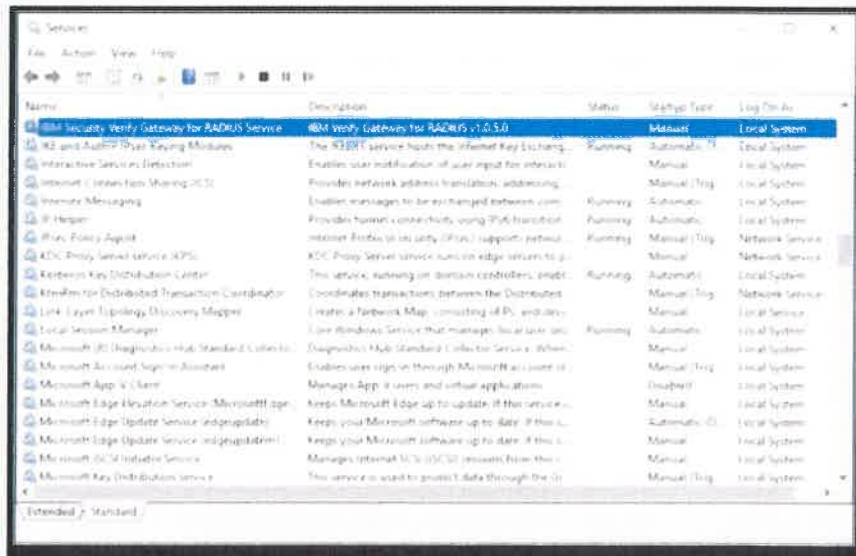
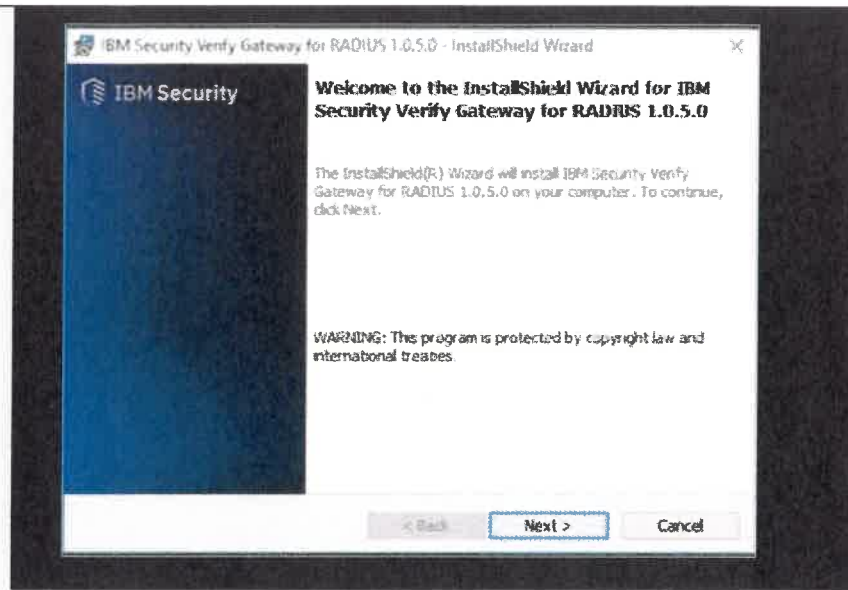
- **Token Management:** IBM Security Verify provides robust token management functionalities, enabling administrators to create, revoke, and manage tokens used for API authentication and authorization.
- **Token Creation:** The platform supports the creation of API tokens through its administrative interface or programmatically via its own APIs. These tokens can be assigned with specific scopes, durations, and permissions, tailoring access control to meet precise requirements.

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

IBM Security Verify offers extensive API capabilities for integration with custom applications and workflows, providing a comprehensive set of RESTful APIs that cover user lifecycle management, authentication, authorization, multi-factor authentication (MFA), and identity governance. These APIs enable customizable integration, allowing for the automation of identity management tasks, the creation of adaptive authentication flows, and fine-grained access control within applications. With support for event hooks and webhooks for real-time notifications, secure API interactions through modern protocols, and extensive documentation and developer tools, IBM Security Verify facilitates the development of secure, responsive applications and workflows that meet complex identity and access management requirements.

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

<p>IBM Security Verify ensures the security and privacy of data transmitted through its Application Programming Interfaces (APIs) by implementing a comprehensive set of security measures. These measures include using HTTPS for secure communication channels, employing OAuth 2.0 and OpenID Connect for secure and token-based authentication, and enforcing strict access control with granular permissions to ensure that only authorized applications and users can access sensitive data. Data encryption in transit and at rest further protects against interception and unauthorized access. Additionally, IBM Security Verify adheres to industry-standard compliance frameworks and best practices for data security and privacy, providing regular security audits, vulnerability assessments, and compliance checks to maintain the highest levels of data protection.</p>	
4.3.1.6.	<p>Can your solution support standards like Open Authorization (OAuth) 2.0 and OpenID Connect for secure Application Programming Interface access?</p>
<p>Yes, IBM Security Verify supports standards like Open Authorization (OAuth) 2.0 and OpenID Connect (OIDC) for secure Application Programming Interface (API) access. These protocols are integral to its security architecture, ensuring that API interactions are authenticated and authorized securely, facilitating token-based access control without exposing user credentials.</p>	
4.3.1.7.	<p>Detail the scalability of your Application Programming Interface infrastructure to support high volumes of authentication and authorization requests.</p>
<p>IBM Security Verify's API infrastructure is designed for scalability and high availability, capable of supporting large volumes of authentication and authorization requests. It employs a cloud-native architecture that automatically scales resources up or down based on demand, ensuring that authentication and authorization services remain responsive and reliable, even during peak usage periods. Load balancing techniques distribute API requests efficiently across multiple servers and instances, minimizing latency and optimizing performance. The infrastructure is built on robust, globally distributed data centers, enhancing its ability to handle high traffic volumes and ensure continuous availability. Additionally, IBM Security Verify's use of advanced caching and optimized session management further improves its scalability, making it well-suited for organizations with demanding, high-volume identity and access management needs.</p>	
4.3.1.8.	<p>Does your solution provide Remote Authentication Dial-In User Service (RADIUS) support that does not require on-premise components?</p>
<p>IBM Security Verify Gateway for RADIUS includes an interface whereby VPNs and other RADIUS clients can request authentication using the multi-factor authentication mechanisms from the IBM Security Verify cloud platform.</p>	



```

{
  "address": ":",
  "port": 20123,
  "trace-file": "c:/tmp/ibm-auth-api.log",
  "ibm-auth-api": {
    "client-id": "h54hhgh-7641-975t-pd58-3857kgu@c21",
    "client-secret": "XXXX-XXXX-XXXX",
    "protocol": "https",
    "host": "mytenant.ice.ibmcloud.com",
    "port": 643,
    "max-handlers": 16
  },
  "clients": [
    {
      "name": "VPN Clients",
      "address": "192.168.1.1",
      "secret": "331922tbjw49h0",
      "auth-method": "password-then-choice-then-otp",
      "otp-prompt": "Enter IBM Verify OTP:",
      "reject-on-missing-auth-method": false,
      "choice-prompt": "I",
      "choice-line-prompt": "{selector: 'X', description: 'XO'}",
      "device-prompt": "A push notification has been sent to your device: [XO]. Refresh your devi",
      "transients-in-choice": true,
      "no-devices-in-choice": false,
      "no-enrollments-in-choice": true,
      "transient-choices": ["emails"],
      "poll-device": true,
      "poll-timeout": 120
    }
  ],
  "policy": [
    {
      "name": "policy1",
      "watch": {
        "apply-before-authenticate": false,
        "client-ip": "172.16.39.46",
        "attr": {
          "case-ignore": true,
          "compare": "=",
          "name": "User-Name",
          "value": "Administrator?"
        }
      }
    }
  ]
}

```

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.

es, IBM Security Verify supports push notifications as a multi-factor authentication method, providing a user-friendly and secure way for users to verify their identity by approving authentication requests on their registered mobile devices. To lower the risk of push fatigue attacks, where users might approve a request without proper scrutiny due to an excessive number of notifications, IBM Security Verify implements several controls:

4.3.1.10. List the Multi-factor methods supported.

IBM Security Verify supports a wide range of multi-factor authentication (MFA) methods to provide enhanced security for user access and transactions. The supported MFA methods include:

- One-Time Password (OTP): Delivered via SMS or email, providing a time-limited code that users must enter along with their regular credentials.
- Mobile Push Notifications: Users receive a push notification on their registered mobile device and approve the authentication request with a single tap.
- Biometric Authentication: Utilizes users' biometric data, such as fingerprint scans or facial recognition, for authentication on supported devices.
- FIDO2 Security Keys: Supports FIDO2-compliant hardware security keys for authentication, offering a high level of security and resistance against phishing attacks.
- Physical Tokens: Traditional hardware tokens that generate a secure code for user authentication.

<p>4.3.1.11.</p>	<p>Does your service offer out of the box login flows that protect against brute-force attacks?</p>
<p>Yes, IBM Security Verify offers out-of-the-box login flows designed to protect against brute-force attacks. These protective measures include account lockout policies, which temporarily disable an account after a predefined number of unsuccessful login attempts, and CAPTCHA challenges that distinguish human users from automated access attempts. Additionally, IBM Security Verify implements rate limiting to control the number of requests from a single source within a certain timeframe, further safeguarding against brute-force attempts. These built-in security features ensure that user accounts remain secure against unauthorized access attempts, enhancing the overall security posture of the organization.</p>	
<p>4.3.1.12.</p>	<p>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.</p>
<p>Yes, IBM Security Verify provides out-of-the-box login flows designed to protect against brute-force attacks. These protections include:</p> <ul style="list-style-type: none"> • Account Lockout Policies: Automatically lock user accounts after a predetermined number of unsuccessful login attempts, preventing further attempts for a specified lockout duration. This mitigates the risk of attackers successfully guessing a user's credentials through repeated attempts. • CAPTCHA Challenges: Deploy CAPTCHA challenges after a certain number of failed login attempts to differentiate between human users and automated access attempts, adding an additional layer of security against automated brute-force attacks. • Rate Limiting: Implement rate limiting on authentication attempts, restricting the number of login requests allowed from a single IP address or user account within a given timeframe. This helps to slow down and deter brute-force attacks by making them time-consuming and resource-intensive for attackers. 	
<p>4.3.1.13.</p>	<p>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.</p>
<p>IBM Security Verify supports a comprehensive range of authentication methods to ensure secure access while providing flexibility to meet various user needs and security policies. These methods include:</p> <ul style="list-style-type: none"> • Email Multi-Factor Authentication (MFA): Sends a one-time passcode or verification link to the user's registered email address, which they must enter or click to complete the authentication process. • SMS MFA: Sends a one-time passcode to the user's mobile phone via text message, which the user then enters to authenticate. 	

- **Biometric Authentication/WebAuthN:** Leverages users' biometric data, such as fingerprints, facial recognition, or voice patterns, for authentication. WebAuthN (Web Authentication API) allows for secure and easy authentication using biometrics or hardware security keys without the need for passwords.
 - **TOTP (Time-based One-Time Password):** Uses applications like Google Authenticator or IBM Verify to generate a time-limited passcode, which the user enters during the authentication process.
 - **Push Notifications:** Sends a push notification to a registered mobile device, where the user can approve or deny the authentication request with a single tap.
 - **FIDO2 Security Keys:** Supports Fast Identity Online (FIDO2) standard, allowing users to use hardware security keys as an authentication method. This method is highly secure and resistant to phishing attacks.
 - **Physical Tokens:** Traditional hardware tokens that generate a secure code for user authentication.
- IBM Security Verify's platform also offers:
- **Adaptive Authentication:** Dynamically adjusts authentication requirements based on the user's context, such as location, device, network, and behavior, enhancing security without compromising user experience.
 - **Risk-Based Authentication:** Evaluates the risk level of each login attempt in real-time and applies appropriate authentication measures based on configurable policies, potentially including denying access or stepping up authentication.
 - **Single Sign-On (SSO):** Allows users to access multiple applications with a single set of credentials, improving the user experience and reducing the need for multiple passwords.

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

IBM Security Verify employs adaptive authentication by performing real-time risk assessments of each login attempt, dynamically adjusting authentication requirements based on the assessed risk. It analyzes contextual factors such as user location, device information, network security, and behavior patterns to calculate a risk score. Based on this score and predefined security policies, IBM Security Verify decides whether to allow access, require additional authentication factors, or deny access for high-risk attempts. This approach enables the solution to provide a seamless user experience for low-risk scenarios while applying stricter verification for higher-risk situations, leveraging technologies like machine learning for behavior analytics and offering a range of step-up authentication methods, including one-time passcodes and biometric verification, to ensure security without compromising user convenience.

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

Yes, IBM Security Verify can integrate with third-party identity providers for federated authentication. This allows organizations to leverage existing identity infrastructures and provide users with seamless access to applications and services across different platforms. IBM Security Verify supports standard federation protocols such as SAML 2.0, OpenID Connect (OIDC), and OAuth 2.0, facilitating secure and straightforward integration with a wide range of identity providers, including popular services like Microsoft Azure AD, Google, and others. This capability enables users to authenticate once and gain access to multiple applications and services without the need for separate login processes, enhancing user experience while maintaining strong security.

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.
------------------	---

IBM Security Verify supports standard federation protocols such as SAML 2.0, OpenID Connect (OIDC), and OAuth 2.0, facilitating secure and straightforward integration with a wide range of identity providers, including popular services like Microsoft Azure AD, Google, and others. This capability enables users to authenticate once and gain access to multiple applications and services without the need for separate login processes, enhancing user experience while maintaining strong security.

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

IBM Security Verify enhances security through adaptive authentication, dynamically adjusting authentication methods based on contextual factors such as location and device. By evaluating real-time information, such as a login attempt from an unusual location or an unrecognized device, IBM Security Verify can identify higher-risk scenarios and respond by requiring additional verification steps like one-time passcodes, biometric checks, or security questions. Conversely, for access attempts from familiar locations and known devices, it may streamline the process with simpler authentication methods.

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

IBM Security Verify effectively addresses scenarios where a user has lost their primary authentication device by providing fallback authentication mechanisms and administrative support. Users are encouraged to register multiple authentication methods upfront, such as a secondary phone, email for OTP, or security questions. In the event of losing their primary device, users can choose an alternative method to verify their identity and gain access. Additionally, IBM Security Verify offers administrative tools that allow system administrators to assist users in these situations by temporarily bypassing the lost device for authentication, resetting the user's primary authentication method, or helping them register a new device.

<p>4.3.1.19.</p>	<p>Can the solution block access based on blacklisted Internet Protocol (IP) addresses or Geogrpahy (GEO) location?</p>
<p>Yes, IBM Security Verify can block access based on blacklisted Internet Protocol (IP) addresses or geography (GEO) location. The solution provides robust access control policies that allow administrators to define and enforce security rules based on various criteria, including the user's IP address and geographic location. By setting up these policies, organizations can prevent access attempts from specific regions or IP ranges known to pose a higher risk or are deemed untrustworthy. This feature is particularly useful in enhancing security by minimizing the potential for unauthorized access from locations associated with malicious activities or outside of the operational boundaries of the organization.</p>	
<p>4.3.1.20.</p>	<p>Does the service identify, detect, and block suspicious authentication activity?</p>
<p>Yes, IBM Security Verify is designed to identify, detect, and block suspicious authentication activity as part of its comprehensive security features. The solution utilizes advanced analytics, behavior analysis, and risk-based authentication mechanisms to continuously monitor authentication attempts. By evaluating various factors such as user behavior patterns, access locations, device integrity, and time anomalies, IBM Security Verify can identify activities that deviate from the norm. When suspicious activity is detected, the system can automatically take predefined actions to mitigate potential security risks, including prompting for additional authentication factors, blocking the authentication attempt, or alerting administrators for further investigation.</p>	
<p>4.3.1.21.</p>	<p>Does the solution perform behavior detection during authentication? (Example: Impossible Travel, Device context, Network Context,)</p>
<p>Yes, IBM Security Verify incorporates behavior detection during authentication to enhance security and detect potential threats. It analyzes behavioral patterns and contexts, such as impossible travel scenarios (logging in from geographically distant locations within an unrealistic timeframe), device context (using a new or unrecognized device), and network context (accessing from an unfamiliar network). By evaluating these and other behavioral indicators, IBM Security Verify can identify anomalies that may suggest fraudulent activity. When such anomalies are detected, the system can trigger additional security measures, such as step-up authentication or alerting administrators, to prevent unauthorized access and ensure the integrity of user accounts. This behavior detection capability is a key component of IBM Security Verify's adaptive authentication approach, allowing it to dynamically adjust security measures based on assessed risk levels.</p>	
<p>4.3.1.22.</p>	<p>How does your platform detect and prevent unauthorized access?</p>
<p>IBM Security Verify detects and prevents unauthorized access through a combination of real-time risk assessments, adaptive authentication, and behavior analysis. It continuously evaluates login attempts and user activities for signs of suspicious behavior, such as impossible</p>	

travel, device and network context anomalies, or deviations from typical user patterns. Based on these assessments, IBM Security Verify dynamically adjusts authentication requirements, potentially escalating to more secure authentication methods like biometric verification or multi-factor authentication (MFA) for higher-risk scenarios. Additionally, it employs machine learning algorithms to improve threat detection over time and can enforce access policies that block access from blacklisted IP addresses or geographical locations. The platform also offers comprehensive logging and monitoring tools, enabling administrators to track and respond to potential security incidents swiftly.

4.3.1.23.

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

Yes, IBM Security Verify supports Attribute-Based Access Control (ABAC) to dynamically adjust access rights based on user attributes. This approach allows for fine-grained access control policies that consider various user attributes, such as role, department, location, and more, in making access decisions. By leveraging ABAC, IBM Security Verify enables organizations to define policies that automatically evaluate and enforce access based on the specific attributes of each user and the context of their access request. This means that access rights can be dynamically adapted in real-time, ensuring that users have access to only the resources necessary for their current task or role, enhancing security and compliance while supporting a seamless user experience.

4.3.1.24.

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

Yes, IBM Security Verify can integrate with external identity providers to extend authorization capabilities. This integration allows organizations to leverage existing identity infrastructures and streamline user access across a wide range of applications and services. By supporting standard protocols such as SAML 2.0, OpenID Connect (OIDC), and OAuth 2.0, IBM Security Verify facilitates seamless federated authentication and authorization with external identity providers. This capability enables a unified access management experience, where users can authenticate once and gain access to all authorized resources, regardless of where those resources reside.

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, IBM Security Verify can enforce access policies based on contextual factors such as time of day, location, and user behavior. This is part of its adaptive and risk-based authentication capabilities, which allow for dynamic access control decisions to be made in real-time. By evaluating these contextual factors, IBM Security Verify can identify potential security risks associated with an access request and adjust the authentication requirements or access permissions accordingly.

<p>4.3.1.26.</p>	<p>Describe your solution's approach to enforcing the principle of least privilege for user access.</p>
<p>IBM Security Verify enforces the principle of least privilege through a blend of role-based access control (RBAC), attribute-based access control (ABAC), and policy enforcement mechanisms. It assigns users to roles with predefined access rights tailored to their job functions, while ABAC considers additional attributes and contextual factors to dynamically adjust permissions. The solution utilizes policy-based controls for precise access decisions, automated provisioning and deprovisioning based on user lifecycle events, and conducts regular access reviews to ensure rights remain aligned with users' needs. This comprehensive approach ensures users are granted only the necessary access for their roles, minimizing the risk of unauthorized access and maintaining a robust security posture.</p>	
<p>4.3.1.27.</p>	<p>How does your platform support session termination and re-authentication based on inactivity or specific triggers?</p>
<p>IBM Security Verify supports session termination and requires re-authentication based on inactivity or specific triggers through configurable session management policies. Administrators can define session timeout intervals, after which inactive sessions are automatically terminated, prompting users to re-authenticate to regain access. Additionally, IBM Security Verify can be configured to monitor for specific events or conditions as triggers for session termination or forced re-authentication. Such triggers could include anomalous behavior, accessing sensitive resources, or changes in the user's risk profile. By implementing these session management and control features, IBM Security Verify ensures that active sessions remain secure and are appropriately managed based on organizational security policies and user activity.</p>	
<p>4.3.1.28.</p>	<p>Does the solution have the ability to have isolated lower environments for the purposes of testing / development?</p>
<p>Yes, IBM Security Verify supports the creation of isolated lower environments for testing and development purposes. This feature allows organizations to safely develop, test, and validate new access policies, integrations, and features without affecting the production environment. These isolated environments can replicate the production setup to ensure accurate testing conditions, but they operate independently to prevent any unintended impacts on live user data and services. By providing these separate environments, IBM Security Verify enables organizations to follow best practices for software development and deployment, such as staging and pre-production testing, thereby ensuring that changes are thoroughly vetted before being rolled out to end-users.</p>	
<p>4.3.1.29.</p>	<p>Does your solution provide multiple environments for testing purposes?</p>
<p>Yes, IBM Security Verify provides multiple environments for testing purposes, enabling organizations to establish isolated settings for development, testing, staging, and production.</p>	

<p>This capability allows for a secure and controlled approach to deploying and testing changes, ensuring that new configurations, policies, and integrations can be thoroughly evaluated in a non-production environment before being implemented in the live environment. These separate environments support best practices in software development and deployment lifecycle management, facilitating risk mitigation and promoting higher quality and stability of identity and access management solutions deployed to end-users.</p>	
<p>4.3.1.30.</p>	<p>Does the solution allow automation of tasks through scripting or Application Programming Interface calls?</p>
<p>Yes, IBM Security Verify allows for the automation of tasks through scripting and Application Programming Interface (API) calls. This capability enables organizations to streamline and automate various identity and access management processes, such as user provisioning and deprovisioning, updating user attributes, managing roles and access rights, and executing security policies. By leveraging IBM Security Verify's comprehensive set of RESTful APIs, administrators and developers can create scripts and integrate with other systems to automate workflows, reduce manual effort, enhance efficiency, and ensure consistency across the identity lifecycle management processes. This automation support is crucial for organizations looking to optimize their IAM operations and improve their security posture with minimal manual intervention.</p>	
<p>4.3.1.31.</p>	<p>Do you offer flexible application integrations such as general Security Assertion Markup Language (SAML), OpenID Connect (OIDC) and Open Authorization (OAuth) connectors?</p>
<p>Yes, IBM Security Verify offers flexible application integrations through support for general Security Assertion Markup Language (SAML), OpenID Connect (OIDC), and Open Authorization (OAuth) connectors. This wide range of integration capabilities enables organizations to securely connect and manage access to various cloud and on-premises applications and services. By utilizing these standards-based connectors, IBM Security Verify facilitates seamless single sign-on (SSO), federated identity management, and secure API access, ensuring a unified and secure user experience across the IT ecosystem. These integration options provide the versatility needed to support diverse application environments and authentication requirements, aligning with modern identity and access management strategies.</p>	
<p>4.3.1.32.</p>	<p>Do you offer deployment assistance, documentation, or training to ensure a smooth transition to your platform?</p>
<p>Yes, IBM Security Verify offers comprehensive deployment assistance, documentation, and training resources to ensure a smooth transition to the platform. Deployment assistance is available to help organizations plan, implement, and optimize their IBM Security Verify solution, including integration with existing systems and migration from legacy identity management systems. IBM provides extensive documentation covering setup, configuration, best practices, and troubleshooting to support self-service and technical understanding of the platform. Additionally, IBM offers a range of training options, including online courses,</p>	

webinars, and customized training sessions, designed to enhance the skills of administrators and end-users and ensure they can effectively use and manage the IBM Security Verify solution.

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, IBM Security Verify can leverage Active Directory (AD) as the Identity Provider (IdP), enabling organizations to integrate their existing AD infrastructure for user authentication and identity management. To facilitate this communication, IBM Security Verify can synchronize with AD through directory connectors or agents that are installed within the organization's network. These connectors or agents serve as the bridge between IBM Security Verify and the on-premises Active Directory, allowing for secure and efficient synchronization of user identities and attributes.

The solution is designed to support real-time or near real-time synchronization of information, ensuring that changes in Active Directory (such as user creation, updates, or deletions) are promptly reflected in IBM Security Verify. This capability enables organizations to maintain consistent and up-to-date identity information across their on-premises and cloud-based systems, supporting seamless access management and authentication processes. The real-time sync feature is crucial for dynamic environments where timely application of access rights and policies based on current user status and attributes is necessary for security and compliance.

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.
------------------	--

When an agent is required to facilitate a connection between Active Directory (AD) and IBM Security Verify, the information exchange is secured through encrypted communication channels. The agent communicates with IBM Security Verify using secure protocols such as HTTPS/TLS, ensuring that all data transferred is encrypted and protected from interception or tampering. Authentication tokens and certificates are used to establish trust and verify the identities of the communicating parties. Additionally, sensitive data, such as passwords, are never directly passed but rather synchronized through secure hashing mechanisms.

For redundancy and failover, IBM Security Verify supports the deployment of multiple agents across different servers or network segments. This distributed architecture ensures that if one agent or its host server encounters issues, others can continue to operate, maintaining the synchronization process without interruption. Load balancing can be implemented to distribute synchronization tasks among available agents, enhancing performance and reliability. In the event of an agent failure, failover mechanisms can automatically reroute tasks to operational agents, ensuring a constant flow of information. Organizations are encouraged

to monitor the health and status of these agents and configure alerts for any operational issues, allowing for prompt response and maintenance to uphold continuous synchronization and access management operations.

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, IBM Security Verify SaaS does support the ability to import password hashes from other Identity Providers (IDPs). This feature is crucial for seamless migration and integration of existing user credentials into the IBM Security Verify platform. Here's a breakdown of how it works and the supported hashing algorithms:

Supported Hashing Algorithms: IBM Security Verify SaaS supports various standard hashing algorithms commonly used in identity management systems. These typically include popular options like SHA-1, SHA-256, SHA-512, and MD5. However, it's essential to check the specific documentation or inquire with IBM for the most up-to-date information on supported algorithms as this can vary over time with advancements in security standards.

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, IBM Security Verify includes an administrator dashboard User Interface (UI) that provides comprehensive tools for managing users and their access rights. Through this dashboard, administrators can easily add, update, and delete user accounts, configure roles and permissions, and set up access policies among other tasks. This centralized management interface enhances visibility and control over the identity and access management processes within the organization.

Moreover, IBM Security Verify allows for the enforcement of specific multi-factor authentication (MFA) types for administrative access. Administrators can configure security policies that require stronger authentication methods for accessing the administrative dashboard or performing sensitive operations. This can include options like biometric verification, one-time passwords (OTP) sent via SMS or email, or push notifications to a mobile app, among others. Enforcing advanced MFA methods for administrators helps bolster security by adding an additional layer of protection against unauthorized access to critical management functions. This approach aligns with best practices for securing privileged accounts and sensitive administrative interfaces

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

Yes, IBM Security Verify supports external federation, enabling organizations to seamlessly integrate with a wide range of external Identity Providers (IdPs). This capability allows users to leverage their existing identities from other systems for authentication, providing a unified access experience across various services and applications. IBM Security Verify utilizes

standard federation protocols, including SAML 2.0, OpenID Connect (OIDC), and OAuth 2.0, to facilitate these integrations.

Through these protocols, IBM Security Verify can federate with numerous IdPs, including but not limited to:

- Microsoft Azure Active Directory (Azure AD)
- Google Identity
- Amazon Web Services (AWS) Cognito
- Okta
- Ping Identity
- OneLogin

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

IBM Security Verify streamlines the user onboarding and offboarding processes through automation, integration capabilities, and policy enforcement. For onboarding, IBM Security Verify automates the creation of user accounts and assignment of access rights based on predefined roles and policies. This can be triggered by events such as a new employee record in the HR system, leveraging integration with HR management systems or directories like Active Directory. The platform ensures that new users receive immediate access to necessary resources and applications according to their role, department, or project needs, enhancing productivity and user experience from day one.

For offboarding, IBM Security Verify automates the revocation of access rights and deactivation of user accounts, which can be initiated by events like an employee's departure in the HR system. The platform ensures that access to corporate resources is promptly removed, minimizing the risk of unauthorized access or data breaches. This automated process is complemented by periodic access reviews and certifications, ensuring that users have only the access they need throughout their tenure.

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

IBM Security Verify implements role-based access control (RBAC) and user provisioning through an integrated and automated framework, designed to efficiently align user access rights with their organizational roles and responsibilities. By defining specific roles associated with distinct access privileges to various applications and data, IBM Security Verify ensures that users automatically inherit the necessary permissions upon being assigned to these roles. This streamlined approach facilitates adherence to the principle of least privilege and simplifies compliance management. Furthermore, the platform automates the lifecycle of user accounts—from creation and updates to deactivation—by integrating with HR systems and directories like Active Directory for real-time data synchronization. This automation not only minimizes manual administrative tasks but also ensures that access rights are accurately and

promptly updated in response to changes in employment status or roles, enhancing security and operational efficiency while providing a seamless user experience.

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

IBM Security Verify provides extensive customization options for the user interface (UI) and branding to ensure that organizations can offer a seamless and cohesive experience that aligns with their corporate identity. These options include the ability to customize branding elements such as logos and color schemes across user-facing interfaces, creation of custom login pages tailored to match organizational branding requirements, and customization of email templates for various communications to maintain consistency with the organization's branding and messaging. Additionally, IBM Security Verify enables the customization of user portals, allowing users to manage their profiles and settings within a branded environment. Localization support further enhances the user experience by allowing customization to accommodate different languages, catering to a global user base. Through these customization capabilities, IBM Security Verify allows organizations to reinforce their brand identity and improve user engagement by providing a personalized and branded access management experience.

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, IBM Security Verify supports the use of multiple Multi-Factor Authentication (MFA) factors for user authentication prior to performing self-service password maintenance tasks, such as resetting a forgotten password, changing an existing password, or unlocking an account. This ensures that even sensitive self-service operations are protected by strong authentication measures, minimizing the risk of unauthorized access. Users can be prompted to authenticate using one or more MFA methods configured within the system—such as SMS-based one-time passcodes, email verification, push notifications, biometric verification, or security questions—before they can proceed with password maintenance actions. This approach reinforces security by verifying the user's identity through multiple factors, thereby providing an additional layer of protection for user accounts and sensitive information.

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?

Yes, IBM Security Verify SaaS typically includes a feature known as "Password Policy Enforcement," which often incorporates the capability to compare supplied new passwords against a database of known-compromised credentials. This feature is commonly referred to as "password screening" or "password blacklist checking."

Here's how this process generally works:

1. **Password Screening:** When a user attempts to reset their password, IBM Security Verify SaaS checks the new password against a database or list of known-compromised credentials. This database is often compiled from various sources, including data breaches, password dumps, and security research.
2. **Blocking Compromised Credentials:** If the new password matches any entry in the database of compromised credentials, IBM Security Verify SaaS blocks the use of that password. This prevents users from selecting passwords that have previously been exposed in security incidents, reducing the risk of account compromise due to reused or easily guessable passwords.
3. **User Notification:** In the event that the user's chosen password is found to be compromised, IBM Security Verify SaaS typically provides feedback to the user, informing them that their password selection is not acceptable due to security reasons. Users are then prompted to choose a different, more secure password.
4. **Continuous Updating:** The database of known-compromised credentials is regularly updated to incorporate new breaches and compromised passwords. This ensures that the password screening feature remains effective against emerging threats and security vulnerabilities.

By implementing password screening functionality, IBM Security Verify SaaS enhances security by proactively preventing the use of compromised credentials, thereby reducing the risk of unauthorized access and data breaches. This feature aligns with best practices in password management and strengthens overall security posture.

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

IBM Security Verify enhances user autonomy and reduces IT administrative workload by offering robust self-service features for password management and profile updates. Users can independently reset forgotten passwords and unlock their accounts by verifying their identity through configurable multi-factor authentication methods, such as SMS verification codes, email links, push notifications, or security questions. Additionally, they have the flexibility to change their current passwords while adhering to organizational security policies directly from a user-friendly self-service portal. This portal also enables users to update their personal profile information, ensuring that contact details and preferences remain up-to-date. Moreover, IBM Security Verify empowers users to manage their multi-factor authentication settings, allowing the addition or removal of authentication methods based on personal preference, thus striking a balance between stringent security measures and user convenience. These self-service capabilities not only streamline the user experience but also significantly decrease the volume of helpdesk tickets related to account and password issues, contributing to overall operational efficiency.

<p>4.3.1.44.</p>	<p>How does your platform handle de-provisioning of user access when an employee leaves the organization?</p>
<p>IBM Security Verify handles the de-provisioning of user access when an employee leaves the organization through automated and policy-driven processes. The platform integrates with HR systems and other authoritative sources of employee status information to trigger de-provisioning actions based on employment status changes. When an employee is marked as leaving the organization in the HR system, IBM Security Verify receives this information and automatically begins the process of revoking access rights across all connected systems and applications.</p> <p>The de-provisioning process is comprehensive and can include disabling the user's account, revoking access to applications and data, and removing the user from groups and roles. This ensures that the departing employee no longer has access to any organizational resources, minimizing the risk of unauthorized access or data breaches post-employment.</p>	
<p>4.3.1.45.</p>	<p>What mechanisms are in place to ensure that user access is granted or revoked promptly?</p>
<p>IBM Security Verify ensures prompt granting and revocation of user access through an integrated approach that combines real-time synchronization, automated provisioning and de-provisioning, policy-driven access controls, and continuous access reviews. By integrating with HR systems and directories like Active Directory for real-time monitoring of changes in employment status or roles, IBM Security Verify can instantly trigger appropriate access adjustments. Automated workflows facilitate the quick provisioning of access for new hires and equally swift de-provisioning when employees leave or change roles, adhering to predefined rules and organizational policies. Access control policies are applied in real-time, ensuring that user access rights are always aligned with the principle of least privilege and current organizational needs. Furthermore, periodic and event-driven access reviews help identify and rectify any inappropriate or outdated access permissions, maintaining a secure and compliant access environment. This comprehensive, policy-driven approach enables IBM Security Verify to manage access rights dynamically and efficiently, ensuring security and compliance across the organization.</p>	
<p>4.3.1.46.</p>	<p>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?</p>
<p>IBM Security Verify integrates with third-party logging and SIEM solutions, offering a robust mechanism for consolidating and analyzing security-related data across the enterprise. It supports exporting logs in versatile formats such as JavaScript Object Notation (JSON), a format well-regarded for its simplicity and compatibility with many SIEM systems, facilitating structured and easily parsable logged events. While JSON is commonly used, IBM Security Verify potentially supports additional formats and integration methods, including APIs and</p>	

webhooks, to enable real-time data streaming to external systems. This real-time capability ensures that security teams have access to the latest logging information, allowing for swift incident response and enhanced security monitoring. Organizations interested in leveraging IBM Security Verify's logging and integration features should consult the most recent documentation or IBM support to understand the full scope of its capabilities, supported formats, and integration best practices, ensuring they maximize their security infrastructure's efficiency and effectiveness.

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.
------------------	---

IBM Security Verify provides a robust suite of reporting capabilities on various authentication statistics and identity management events, catering to the needs of organizations for in-depth security and operational analysis. The solution offers detailed reports on Single Sign-On (SSO) attempts, Multi-Factor Authentication (MFA) enrollment, new user creations, account lockouts, permission changes, and password resets. These insights are crucial for monitoring user access patterns, understanding security posture, and identifying potential issues or vulnerabilities within the authentication process. Beyond these specific metrics, IBM Security Verify also supports custom reporting, allowing organizations to tailor reports to their unique requirements. Real-time alerts and notifications can be configured for immediate awareness of critical events, enhancing the organization's ability to respond swiftly to potential security incidents. Comprehensive audit trails and historical logs support forensic analysis and compliance efforts, while interactive dashboards provide a visual overview of key performance indicators and trends. This combination of detailed reporting, customizable analytics, and real-time monitoring makes IBM Security Verify a powerful tool for maintaining security, ensuring compliance, and optimizing user access management processes.

4.3.1.48.	How long are the logs maintained?
------------------	-----------------------------------

IBM Security Verify SaaS typically manages logging and audit information through a comprehensive logging and auditing framework designed to provide visibility into system activities, user actions, and security events. Here's an overview of how IBM Security Verify SaaS manages logging and audit information:

1. **Logging Infrastructure:** IBM Security Verify SaaS incorporates a robust logging infrastructure that captures a wide range of system activities and events. This includes user authentication events, access control decisions, configuration changes, administrative actions, and security-related incidents.
2. **Event Collection:** Various components within IBM Security Verify SaaS continuously generate logs and audit trails as users interact with the system, access resources, and

perform administrative tasks. These events are collected centrally to ensure centralized visibility and control over system activities.

3. **Audit Policies:** IBM Security Verify SaaS allows administrators to define audit policies and configurations to specify which types of events should be logged and monitored. Administrators can customize audit policies based on organizational requirements, compliance mandates, and security best practices.
4. **Real-time Monitoring:** The logging and audit infrastructure in IBM Security Verify SaaS often supports real-time monitoring and alerting capabilities. Administrators can configure alerts to be triggered for specific events or conditions of interest, enabling timely detection and response to security incidents.
5. **Retention and Storage:** IBM Security Verify SaaS typically provides options for configuring the retention and storage of log data. Administrators can define retention periods based on organizational policies, compliance requirements, and storage capacity considerations. Additionally, IBM may offer options for long-term storage or archival of audit logs for historical analysis and compliance purposes.
6. **Access Controls:** Access to logging and audit information within IBM Security Verify SaaS is typically governed by access controls and permissions. Administrators can define roles and privileges to restrict access to log data to authorized personnel only, helping to maintain the confidentiality and integrity of audit information.
7. **Integration with SIEM Solutions:** IBM Security Verify SaaS often supports integration with Security Information and Event Management (SIEM) solutions, allowing organizations to aggregate, correlate, and analyze log data from IBM Security Verify SaaS alongside data from other security and IT systems. This integration enhances threat detection, incident response, and compliance reporting capabilities.

Overall, IBM Security Verify SaaS employs a comprehensive approach to logging and audit management to help organizations maintain visibility, compliance, and security across their identity and access management environments.

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

IBM Security Verify provides robust reporting capabilities designed to meet the diverse needs of organizations, including executive-level oversight. With a variety of pre-defined report templates, organizations can easily generate reports on authentication statistics, user activities, security incidents, and compliance adherence, catering to both operational and strategic analysis. Additionally, IBM Security Verify offers extensive customization options for reports, allowing organizations to tailor the content and format to specific requirements, ensuring that executives receive targeted, actionable insights. These custom reports can focus on summarizing key security metrics, highlighting trends, identifying risks, and evaluating the effectiveness of the identity and access management framework, all presented in an accessible

format suitable for strategic decision-making. For those seeking detailed, up-to-date information on IBM Security Verify's reporting capabilities, including executive report templates, consulting the latest IBM documentation or contacting IBM support is advisable, ensuring access to current features and best practices in reporting.

4.3.1.50.

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

Below is the list that include but not limited to the security events captured by proposed solution.

the types of security events typically captured and monitored by such platforms:

1. User Authentication Events:

- Successful user logins.
- Failed login attempts (including reasons for failure, such as incorrect credentials or account lockouts).
- Password changes and resets.
- Multi-factor authentication (MFA) events (e.g., successful MFA challenges).

2. User Access Events:

- Access to sensitive resources or applications.
- Unauthorized access attempts.
- Role and permission changes.
- User session management (e.g., session creation, termination, and timeouts).

3. Administrative Actions:

- Changes to user accounts (e.g., creation, deletion, modification).
- Changes to group memberships.
- Configuration changes to the IAM system (e.g., policy updates, security settings).

4. Security Policy Violations:

- Violations of password policies (e.g., use of weak passwords, password sharing).
- Access policy violations (e.g., attempting to access unauthorized resources).
- Policy enforcement actions (e.g., blocking access, requiring additional authentication).

5. Security Threats and Anomalies:

- Detection of suspicious login patterns or behaviors.

- Alerts for potential security threats (e.g., brute-force attacks, phishing attempts).
- Anomaly detection (e.g., unusual access from unfamiliar locations or devices).

6. Audit Trail Events:

- Record of all system activities and changes.
- Timestamps for when events occurred.
- Details of the user or entity responsible for each action.

7. Compliance-related Events:

- Events relevant to regulatory compliance requirements (e.g., GDPR, HIPAA, SOX).
- Evidence of adherence to security policies and standards.

4.3.1.51.

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

IBM Security Verify SaaS provides robust logging mechanisms to capture identity-related events and activities, offering organizations visibility into user authentication, access, and administrative actions. These logging mechanisms are crucial for monitoring and auditing identity-related activities, detecting security threats, and ensuring compliance with regulatory requirements. Here's an explanation of the logging mechanisms typically employed by IBM Security Verify SaaS:

- 1. Event Logging:** IBM Security Verify SaaS generates logs for various identity-related events, including user authentication, access attempts, administrative actions, and policy enforcement. Each event is recorded with relevant details such as the event type, timestamp, user ID, IP address, and outcome (success or failure).
- 2. Centralized Logging Repository:** All identity-related logs are centralized within IBM Security Verify SaaS, providing a single point of access for monitoring and analysis. This centralized logging repository enables organizations to easily search, filter, and analyze log data to identify security incidents, investigate anomalies, and track user activity.
- 3. Real-time Logging:** IBM Security Verify SaaS supports real-time logging, ensuring that identity-related events are captured and logged as they occur. Real-time logging enables organizations to respond promptly to security incidents, mitigate risks, and enforce security policies effectively.
- 4. Customizable Logging Policies:** Organizations can customize logging policies within IBM Security Verify SaaS to specify which identity-related events should be logged and retained. This flexibility allows organizations to tailor logging settings to their specific security and compliance requirements, ensuring that critical events are captured while minimizing unnecessary logging overhead.

- 5. **Integration with SIEM Solutions:** IBM Security Verify SaaS integrates with Security Information and Event Management (SIEM) solutions, allowing organizations to export identity-related logs to their existing SIEM platforms for centralized monitoring, correlation, and analysis. This integration enables organizations to leverage their existing SIEM investments and consolidate security monitoring efforts.
- 6. **Encryption and Data Protection:** Identity-related logs stored within IBM Security Verify SaaS are encrypted and protected using industry-standard encryption algorithms and security measures. This ensures the confidentiality and integrity of log data, guarding against unauthorized access and tampering.
- 7. **Retention and Archiving:** IBM Security Verify SaaS allows organizations to configure retention and archiving policies for identity-related logs, specifying the duration for which logs should be retained and archived. This enables organizations to comply with regulatory requirements and retain historical log data for forensic analysis and audit purposes.

Overall, the logging mechanisms in place within IBM Security Verify SaaS provide organizations with comprehensive visibility into identity-related events and activities, empowering them to maintain security, detect threats, and demonstrate compliance with confidence.

4.3.1.52.

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

IBM Security Verify delivers real-time alerts for security incidents and policy violations through advanced monitoring, analytics, and policy enforcement mechanisms. The platform analyzes user behaviors and security events continuously, utilizing machine learning to detect anomalies that could indicate security risks. Administrators can define custom security policies that, when breached, trigger immediate alerts. These alerts, containing detailed incident information, are promptly delivered to security teams via preferred channels such as email or SMS, or integrated into third-party SIEM systems for a comprehensive security overview. This approach ensures that security personnel are immediately aware of potential threats, enabling swift action to mitigate risks and uphold the organization's security posture.

4.3.1.53.

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

IBM Security Verify effectively supports compliance requirements through the generation of detailed audit trails and activity reports, capturing a wide array of user actions, authentication events, and system changes. This capability is crucial for adhering to various regulatory frameworks such as GDPR, HIPAA, and SOC 2, among others. The platform enables organizations to customize and export reports tailored to specific compliance needs, providing essential evidence of effective security controls and access management practices. With IBM Security Verify, organizations can engage in real-time monitoring and historical analysis, facilitating proactive compliance management and the ability to respond confidently to audit

<p>inquiries. This comprehensive approach ensures that organizations can meet their compliance obligations while maintaining a high standard of security.</p>	
<p>4.3.1.54.</p>	<p>What options are available for exporting logs and reports to external systems or Security information and event management (SIEM) solutions?</p>
<p>IBM Security Verify offers versatile options for exporting logs and reports to external systems or SIEM solutions, enhancing organizations' ability to integrate identity and access management insights into their broader security operations. Through RESTful APIs, IBM Security Verify facilitates programmatic retrieval of detailed logs and reports, allowing for direct integration with external systems. For real-time or near-real-time log streaming, Syslog forwarding is supported, enabling immediate analysis and response. Additionally, IBM Security Verify can directly integrate with leading SIEM solutions via pre-built connectors, streamlining the ingestion of crucial security data. For organizations with specific data processing needs, logs and reports can also be exported in common file formats like CSV or JSON, offering flexibility in how data is analyzed and used within external systems. This comprehensive approach ensures that IBM Security Verify's identity and access management data can significantly contribute to an organization's overall security and compliance posture, providing valuable insights for detecting and responding to potential security threats.</p>	
<p>4.3.1.55.</p>	<p>Indicate and identify any countries where you provide services to clients outside of the United States (and US territories).</p>
<ul style="list-style-type: none"> • IBM Security Verify is a versatile product developed by IBM, designed to cater to a diverse range of industries across the globe. Its application spans various sectors, including healthcare, finance, education, and government, underscoring its adaptability and the trust it has garnered internationally. • SPS Inc. has helped customers outside US implement IAM including UAE, Germany, Pakistan, and Bahrain. 	
<p>4.3.1.56.</p>	<p>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</p>
<p>No security breaches were recorded or reported.</p>	
<p>4.3.1.57.</p>	<p>Provide information on how clients are informed of maintenance and patch releases.</p>
<p>IBM Security Verify ensures clients are well-informed of maintenance and patch releases through a comprehensive communication strategy that encompasses email notifications, a dedicated service dashboard, detailed release notes and documentation, direct support channels, and community forums and social media. Email notifications provide advance notice and details of the updates, while the service dashboard offers real-time status updates and maintenance schedules. Release notes and updated documentation offer an in-depth look at</p>	

the changes and enhancements. For any inquiries or concerns, IBM's support team is readily accessible, and community forums and social media platforms serve as additional resources for updates and engagement. This multifaceted approach guarantees that clients have all the necessary information to prepare for and adapt to maintenance and patch releases, minimizing any impact on their operations.

4.3.1.58.	Where does the solution reside?
------------------	---------------------------------

IBM Security Verify is a cloud-based solution, residing in IBM's secure cloud infrastructure. This setup allows for a scalable, flexible, and reliable service that can be accessed from anywhere, offering organizations the benefits of a cloud-native identity and access management (IAM) platform. The cloud-based nature of IBM Security Verify enables rapid deployment, ease of management, and automatic updates, ensuring that clients always have access to the latest features and security enhancements without the need for extensive on-premise infrastructure. IBM provides robust data centers globally, ensuring compliance with regional data privacy regulations and standards, and offering clients options to select data residency according to their geographical and regulatory needs.

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.
------------------	--

Ensuring compliance with accessibility standards such as the Americans with Disabilities Act (ADA) is crucial for IBM Security Verify SaaS to ensure that its platform is usable by individuals with disabilities. Here's how IBM typically supports ADA standards and facilitates accessibility, including support for screen readers and descriptive technology:

1. **Accessibility Features:** IBM Security Verify SaaS is designed with accessibility features built into its user interface. These features are intended to make the platform navigable and usable by individuals with disabilities, including those who rely on screen readers and other assistive technologies.
2. **Screen Reader Compatibility:** IBM typically ensures that the user interface of Security Verify SaaS is compatible with popular screen reader software such as JAWS (Job Access With Speech), NVDA (NonVisual Desktop Access), and VoiceOver. This compatibility enables individuals with visual impairments to access and interact with the platform effectively.
3. **Keyboard Navigation:** IBM Security Verify SaaS typically supports keyboard navigation as an alternative input method for users who cannot use a mouse or other pointing device. This ensures that individuals with mobility impairments can navigate the platform and perform tasks using keyboard shortcuts and commands.
4. **Descriptive Technology:** IBM typically incorporates descriptive technology within the user interface of Security Verify SaaS to provide informative and descriptive elements that assist users in understanding the content and functionality of the platform. This

includes descriptive text for images, icons, and other visual elements to ensure that users with visual impairments can interpret and interact with them effectively.

5. **Accessibility Standards Compliance:** IBM typically ensures that Security Verify SaaS complies with recognized accessibility standards, including the Web Content Accessibility Guidelines (WCAG) published by the World Wide Web Consortium (W3C). These standards provide guidelines and best practices for creating accessible web content and applications, including recommendations for ensuring compatibility with assistive technologies.
6. **User Feedback and Testing:** IBM typically solicits feedback from users with disabilities and conducts accessibility testing to identify and address any usability barriers or issues within Security Verify SaaS. This iterative process helps to continuously improve the accessibility of the platform and ensure that it meets the needs of all users, regardless of disability.

By incorporating these features and practices, IBM aims to ensure that Security Verify SaaS is accessible to individuals with disabilities, in compliance with ADA standards and other accessibility regulations.

4.3.1.60.

Describe how your service provides failover and redundancy.

IBM Security Verify SaaS typically implements robust failover and redundancy mechanisms to ensure high availability and reliability of the service. Here's how IBM typically provides failover and redundancy within the IBM Security Verify SaaS platform:

1. **Multi-Data Center Architecture:** IBM Security Verify SaaS often operates across multiple geographically distributed data centers. This architecture enhances fault tolerance and ensures redundancy by replicating critical components and data across multiple locations. In the event of a failure or outage in one data center, traffic can be automatically rerouted to alternate data centers to maintain service availability.
2. **Load Balancing:** IBM Security Verify SaaS typically employs load balancers to distribute incoming traffic across multiple servers or instances within each data center. Load balancing helps optimize resource utilization and ensures that no single server or instance becomes overloaded, reducing the risk of service degradation or downtime due to traffic spikes or hardware failures.
3. **Automatic Failover:** IBM Security Verify SaaS often implements automatic failover mechanisms to detect and respond to failures in real-time. When a failure is detected, such as a server or network outage, traffic is automatically redirected to redundant components or backup systems to maintain uninterrupted service availability. This automated failover process helps minimize downtime and ensures seamless continuity of service for users.
4. **Data Replication and Backup:** Critical data within IBM Security Verify SaaS is typically replicated and backed up across multiple storage systems or data centers. This ensures data integrity and availability in the event of hardware failures, data corruption, or

other unforeseen incidents. Regular backups are performed to create redundant copies of data, allowing for rapid recovery in case of data loss or corruption.

5. **Highly Available Infrastructure Components:** IBM typically deploys redundant hardware and infrastructure components within each data center, including servers, networking equipment, and storage systems. Redundant power supplies, network connections, and storage arrays help mitigate the impact of hardware failures and ensure continuous operation of the platform.
6. **Continuous Monitoring and Alerting:** IBM Security Verify SaaS typically employs comprehensive monitoring and alerting systems to continuously monitor the health and performance of the platform. Any deviations from normal operation, such as resource utilization spikes or service disruptions, trigger immediate alerts to operations teams, enabling proactive intervention and remediation to prevent or minimize downtime.

By implementing these failover and redundancy mechanisms, IBM Security Verify SaaS aims to provide customers with a highly available and reliable identity and access management solution, capable of withstanding hardware failures, network outages, and other potential disruptions while maintaining uninterrupted service delivery.

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

IBM Security Verify SaaS typically incorporates a variety of controls and security measures to prevent automated attacks and unauthorized access attempts. Here are some common controls that IBM Security Verify SaaS may have in place:

1. **Rate Limiting:** IBM Security Verify SaaS often implements rate-limiting mechanisms to restrict the number of requests that can be made within a certain time frame. By limiting the rate of requests, the platform can mitigate the risk of brute-force attacks and other automated attacks that rely on rapidly sending a large volume of requests to exploit vulnerabilities or guess credentials.
2. **CAPTCHA Challenges:** IBM Security Verify SaaS may incorporate CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) challenges as a means of distinguishing between legitimate users and automated bots. CAPTCHA challenges typically require users to complete a task, such as identifying objects in images or solving puzzles, before proceeding with their authentication or access request.
3. **Multi-factor Authentication (MFA):** IBM Security Verify SaaS often supports multi-factor authentication (MFA) as an additional layer of security beyond passwords. MFA requires users to provide multiple forms of verification, such as a one-time passcode sent to their mobile device or biometric authentication, reducing the effectiveness of automated attacks that rely solely on compromised credentials.

- 4. **IP Blocking and Whitelisting:** IBM Security Verify SaaS may offer IP blocking and whitelisting capabilities to control access based on IP addresses. Administrators can configure rules to block or allow access from specific IP addresses or ranges, effectively mitigating automated attacks originating from known malicious IP addresses or unauthorized sources.
- 5. **Behavioral Analysis and Anomaly Detection:** IBM Security Verify SaaS often incorporates behavioral analysis and anomaly detection capabilities to identify suspicious patterns or activities indicative of automated attacks. By monitoring user behavior and system activity, the platform can detect deviations from normal behavior and trigger alerts or security measures to prevent unauthorized access attempts.
- 6. **Web Application Firewall (WAF):** IBM Security Verify SaaS may leverage a web application firewall (WAF) to filter and monitor incoming web traffic, blocking malicious requests and known attack vectors before they reach the application. WAFs can help protect against common automated attacks, such as SQL injection, cross-site scripting (XSS), and remote code execution.
- 7. **Security Headers and Secure Configuration:** IBM Security Verify SaaS typically employs security headers and follows secure configuration best practices to enhance resilience against automated attacks. This may include implementing HTTP security headers such as Content Security Policy (CSP), Strict-Transport-Security (HSTS), and X-Frame-Options to prevent common attack vectors and enforce secure communication protocols.

These controls and security measures work together to strengthen the defenses of IBM Security Verify SaaS against automated attacks, helping to safeguard sensitive data, protect user accounts, and maintain the integrity and availability of the platform.

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

IBM Security Verify ensures high availability and resilience through a comprehensive strategy that includes leveraging IBM's global network of data centers for geographic redundancy, implementing advanced load balancing and automatic failover mechanisms, and conducting regular data replication and backups. This approach guarantees that services remain available and data integrity is maintained even during unexpected outages or disasters. The solution's cloud-native, scalable architecture allows for quick adjustments to demand and server capacity, ensuring consistent performance. Additionally, IBM Security Verify benefits from continuous monitoring and a proactive incident response system, manned by IBM's expert security and operations teams. Together, these measures provide a robust foundation for IBM Security Verify, offering clients a reliable and secure identity and access management solution capable of withstanding a wide range of potential disruptions.

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

IBM Security Verify implements a thorough data backup and recovery strategy designed to protect against data loss, ensuring clients' data integrity and service continuity. This strategy encompasses regular, automated data backups stored in encrypted form across secure, geographically distributed data centers, providing both redundancy and resilience. The use of IBM's global data center network ensures that backups are not only frequent but also benefit from geographic redundancy, enhancing disaster recovery capabilities. Data is encrypted during both storage and transfer, safeguarding it from unauthorized access. The solution employs versioning and adheres to specific retention policies, enabling precise recovery from various points in time. Comprehensive disaster recovery planning, which is regularly tested and updated, outlines swift data recovery and system restoration procedures to minimize operational downtime. Additionally, continuous monitoring of the backup and recovery infrastructure ensures its readiness and effectiveness, securing client data against a range of potential disruptions and loss scenarios. Through these meticulous measures, IBM Security Verify maintains high levels of data security and availability, supporting clients' operational resilience.

4.3.1.64.

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

IBM Security Verify's approach to continuous monitoring and threat detection within its identity infrastructure is built on a foundation of real-time analysis, leveraging advanced analytics and machine learning to proactively identify and respond to potential threats. This comprehensive strategy ensures immediate awareness of suspicious behaviors or anomalies, such as compromised credentials or insider threats, by establishing normal behavioral baselines and detecting deviations. The platform employs predefined security policies and risk scoring to assess and mitigate risks promptly, integrating seamlessly with an organization's broader security ecosystem for enhanced visibility and correlated threat detection. Additionally, IBM Security Verify enforces compliance with organizational policies and regulatory standards, while facilitating efficient incident response and remediation workflows. This multifaceted approach not only supports early threat detection but also promotes a proactive security posture, ensuring the integrity and resilience of the identity infrastructure against evolving security challenges.

4.3.1.65.

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

IBM Security Verify employs advanced analytics and user behavior analysis to provide critical insights into anomalies that might indicate compromised accounts. By establishing and monitoring baseline behaviors for users, the platform effectively identifies deviations such as unusual access patterns, login times, or locations, which could suggest account compromise. When such anomalies are detected, IBM Security Verify generates real-time alerts, furnishing security teams with detailed information for swift investigation and response. Leveraging machine learning, the solution continually enhances its ability to discern between normal and anomalous activities, improving the accuracy of identifying potential threats. This proactive

detection and alerting mechanism plays a pivotal role in early identification of compromised accounts, allowing organizations to promptly address security vulnerabilities and maintain a robust defense against unauthorized access.

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

IBM Security Verify employs a comprehensive security approach to ensure data integrity and protect against unauthorized modifications of user attributes. This includes implementing strict role-based and attribute-based access controls to define precise access permissions, ensuring only authorized personnel can modify user data. Data encryption, both at rest and in transit, serves as a critical line of defense, making user attributes unreadable to unauthorized parties. Continuous monitoring and anomaly detection capabilities alert administrators to any suspicious activities, further safeguarding data integrity. Detailed audit trails and logging of all actions related to user attributes provide transparency and facilitate forensic investigations if needed. Additionally, IBM Security Verify undergoes regular security assessments and compliance checks, ensuring adherence to the latest security standards and best practices. Together, these measures form a robust framework for protecting user data against unauthorized access and modifications, reinforcing the overall security posture of organizations using IBM Security Verify.

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

IBM Security Verify allows for the configuration of session timeouts to enhance security by automatically ending sessions after specified periods of inactivity or elapsed time. Administrators can tailor session timeout settings to align with organizational security policies, including idle timeout durations to terminate sessions after a period of inactivity, and absolute timeouts to limit the maximum session duration regardless of activity. Additional configurable parameters may include warning periods to alert users before timeouts, options for session extension to maintain user convenience, and re-authentication requirements for continued access post-timeout. These configurations help prevent unauthorized access from unattended sessions, ensuring a secure and compliant operational environment. Adjusting these settings allows organizations to strike a balance between strict security measures and user experience, catering to the specific needs and risk profiles of different user groups and applications.

4.3.1.68. Are sessions cleared upon logging off?

Yes, in IBM Security Verify, sessions are cleared upon logging off. When a user logs off, the session termination process involves invalidating the session token and clearing session-related data from the server. This ensures that no residual data from the session can be accessed or misused after the user has logged out, providing an additional layer of security. The process of clearing sessions upon logout is a standard security practice to prevent unauthorized access and protect user data, and it is an integral part of IBM Security Verify's

<p>approach to maintaining a secure and trustworthy identity and access management environment.</p>	
<p>4.3.1.69.</p>	<p>Can active user sessions be forcibly terminated by administrators?</p>
<p>Yes, in IBM Security Verify, administrators have the capability to forcibly terminate active user sessions. This feature is crucial for maintaining security and compliance, allowing administrators to respond quickly to potential security threats, breaches, or policy violations by immediately revoking access for specific users. Administrators can use the IBM Security Verify management console to identify active sessions and terminate them as needed, ensuring that unauthorized access can be swiftly curtailed. This ability to manage and control active sessions enhances the overall security posture of the organization, providing administrators with the tools necessary to protect sensitive information and comply with regulatory requirements.</p>	
<p>4.3.1.70.</p>	<p>Describe your approach to managing long-running sessions</p>
<p>IBM Security Verify typically manages long-running sessions through various mechanisms aimed at balancing security and user convenience. Here's how IBM Security Verify typically handles long-running sessions:</p> <ol style="list-style-type: none"> 1. Session Timeout Policies: IBM Security Verify often allows administrators to configure session timeout policies to specify the maximum duration of user sessions. These policies define how long a user can remain inactive before being automatically logged out of the system. By enforcing session timeouts, IBM Security Verify mitigates the risk of unauthorized access due to prolonged periods of inactivity. 2. User Activity Monitoring: IBM Security Verify may incorporate user activity monitoring capabilities to track user interactions and detect suspicious behavior during long-running sessions. Continuous monitoring helps identify potential security threats or unauthorized activities, allowing administrators to intervene promptly and take appropriate action to mitigate risks. 3. Idle Session Management: IBM Security Verify may implement idle session management features to monitor user activity in real-time and automatically log out inactive users after a predefined period of inactivity. This helps prevent unauthorized access to sensitive resources in case users forget to log out or become inactive for an extended period. 4. Session Revocation and Termination: IBM Security Verify typically provides administrators with the ability to revoke or terminate active user sessions manually if necessary. In situations where suspicious activity or security incidents are detected, administrators can take immediate action to invalidate existing sessions and force users to reauthenticate, reducing the potential impact of security breaches. 5. Single Sign-On (SSO) Integration: If IBM Security Verify is integrated with a single sign-on (SSO) solution, it may inherit session management capabilities from the SSO 	

provider. This allows for consistent session management across multiple applications and systems, ensuring that long-running sessions are handled uniformly and according to established policies.

6. **Token-based Authentication:** In scenarios where IBM Security Verify utilizes token-based authentication mechanisms, session management may be handled through the expiration and renewal of authentication tokens. Tokens typically have finite lifetimes and are automatically refreshed or invalidated after a certain period, reducing the risk of session hijacking or unauthorized access.

7. **Secure Communication Protocols:** IBM Security Verify typically employs secure communication protocols, such as HTTPS, to encrypt data exchanged between users' devices and the platform's servers during long-running sessions. This helps protect sensitive information from interception or eavesdropping by malicious actors.

By implementing these session management mechanisms, IBM Security Verify aims to strike a balance between user convenience and security, ensuring that long-running sessions are actively monitored, controlled, and secured to mitigate the risk of unauthorized access and protect sensitive data.

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

IBM Security Verify manages user sessions across various locations by incorporating a sophisticated mix of geo-location analysis, risk-based authentication, adaptive access policies, and continuous monitoring. The platform dynamically adjusts authentication requirements when users access applications from new or unusual locations, enhancing security through additional verification steps. Adaptive access policies take into account the context of each access attempt, including location, device used, and network security, to appropriately grant or restrict access. IBM Security Verify also implements session timeouts and re-authentication mechanisms, especially for sessions initiated from less secure or unfamiliar locations, to further safeguard user sessions. Continuous monitoring and anomaly detection help identify and mitigate potential security risks, such as unusual access patterns, by automatically terminating suspicious sessions and alerting administrators. Additionally, the solution's single sign-on (SSO) and centralized session management capabilities ensure a seamless user experience across multiple applications, without compromising on security.

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

IBM Security Verify empowers administrators with robust tools and capabilities to remotely terminate active user sessions as needed. Through its session management dashboard, administrators gain real-time visibility into active sessions across applications and devices, allowing them to monitor user activities closely. The platform enables granular control over session termination, giving administrators the flexibility to revoke sessions for individual users, specific devices, or all devices associated with a user account. Automated policies can be

configured to proactively manage sessions, such as terminating inactive sessions or based on predefined criteria. Integration with access control policies ensures that session termination aligns with overall access management practices and compliance requirements. Real-time alerts and comprehensive audit logging further enhance security by providing timely notifications of suspicious activities and maintaining detailed records of session management actions. Overall, IBM Security Verify equips administrators with the tools they need to swiftly and securely terminate active sessions, contributing to a robust security posture and effective access management.

4.3.1.73.	Does your solution integrate with Active Roles Server?
------------------	--

IBM Security Verify typically focuses on providing identity and access management capabilities, including user provisioning, access certification, and governance. While it may integrate with various identity and access management (IAM) solutions and directories, such as Microsoft Active Directory, it doesn't natively integrate with Active Roles Server, which is a separate IAM solution primarily focused on Active Directory management and administration.

However, integration between IBM Security Verify and Active Roles Server could potentially be achieved through custom development or middleware solutions. Organizations may leverage APIs, connectors, or identity management platforms to facilitate data synchronization, provisioning workflows, and access controls between the two systems.

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

It adheres to industry standards like SOC 2 and utilizes strong access controls, data encryption, and audit logging to safeguard user information. Additionally, the platform offers features to manage user consent and implement purpose-based privacy rules, which helps organizations comply with regulations like GDPR and CCPA. Overall, IBM Security Verify's commitment to certifications, security controls, and privacy-focused functionalities helps ensure user data remains protected.

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
------------------	---

Following are the three references of clients with similar requirements and user base:

1. **Montgomery College**
 Address: 9221 Corporate Blvd, Rockville, MD 20850
 Contact Person: Moeen Taj/moeen.taj@montgomerycollege.edu
 Number of Users: 50,000

2. **University of Nevada, Las Vegas**
 Address: 4505 S. Maryland Parkway, Las Vegas, NV 89154-1033

Contact Person: Nick Scheib / nscheib@gmail.com

Number of Users: 35,000

3. Asplundh

Address: 708 Blair Mill Road Willow Grove, PA 19090

Contact Person: George Gunther/ggunther@asplundh.com

Number of Users: 40,000

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.

Yes, to fulfill the State of West Virginia's SOC1 requirements, SPS Inc. will provide SSAE No. 18 SOC 1 Type 2 report results on an annual basis. This ensures ongoing compliance with the state's stringent standards for financial reporting and controls. By delivering these reports yearly, SPS Inc. will demonstrate its commitment to maintaining high levels of internal controls and operational effectiveness, aligning with the state's objectives for transparency and accountability in service provision.

References:

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

Reference 1	
Company Name	Montgomery College
Street Address	9221 Corporate Blvd
City, State, Zip Code	Rockville, MD 20850
Contact Person/E-mail	Moeen Taj/moeen.taj@montgomerycollege.edu
Title	Enterprise Application Services Manager
Telephone Number	(240) 687-4385
Service Dates	2021-present
No. of Users	50,000

Reference 2	
Company Name	University of Nevada, Las Vegas
Street Address	4505 S. Maryland Parkway
City, State, Zip Code	Las Vegas, NV 89154-1033
Contact Person/E-mail	Nick Scheib / nscheib@gmail.com
Title	Chief Information Officer
Telephone Number	702-674-6425
Service Dates	2014-2022
No. of Users	35,000

Reference 3	
Company Name	Asplundh
Street Address	708 Blair Mill Road Willow Grove, PA 19090
City, State, Zip Code	Willow Grove, PA 19090
Contact Person/E-mail	George Gunther/ ggunther@asplundh.com
Title	Chief Information Officer
Telephone Number	215-784-4429
Service Dates	2013 – Present
No. of Users	40,000

Identity Management Single Sign-On Training Program

Introduction:

In recognition of the critical role played by the various teams involved in the IAM solution at West Virginia Department of Administration, we propose a tailored training program aimed at equipping the Identity and Access Management, Service Desk, Security, Platform Engineering, and UNIX teams with the necessary skills and knowledge for efficient management, administration, monitoring, troubleshooting, and ongoing maintenance of the new Identity Management System.

Training Objectives:

The training program is designed with the following key objectives in mind:

1. **Comprehensive Understanding:**
 - Develop a thorough understanding of the IAM solution's architecture, components, and integration points.
2. **Role-Specific Proficiency:**
 - Equip each team with role-specific skills tailored to their responsibilities within the IAM ecosystem.
3. **Efficient Management:**
 - Foster the ability to efficiently manage user identities, access controls, and associated policies.
4. **Proactive Monitoring:**
 - Enable proactive monitoring of the IAM solution to identify and address potential issues before they impact operations.
5. **Effective Troubleshooting:**
 - Develop troubleshooting skills to swiftly address challenges and minimize downtime.
6. **Ongoing Maintenance:**
 - Provide expertise in the ongoing maintenance of the Identity Management System, ensuring its continued optimal performance.

Proposed Training Courses:

The following list outlines the proposed training courses tailored to meet the specific needs of each team:

1. **Identity and Access Management Team:**
 - IAM Fundamentals
 - User Lifecycle Management
 - Access Control and Permissions
 - Single Sign-On (SSO) Implementation
 - Multi-Factor Authentication (MFA) Best Practices
2. **Service Desk Team:**
 - End-User Support in IAM

- Troubleshooting Access Issues
 - Password Management
 - Basic IAM Security Awareness
3. **Security Team:**
- IAM Security Best Practices
 - Threat Intelligence Integration
 - Incident Response in IAM
 - Access Control Auditing
4. **Platform Engineering Team:**
- IAM Solution Integration with Existing Systems
 - Infrastructure Requirements and Optimization
 - Scalability Planning
 - High Availability and Disaster Recovery
5. **UNIX Team:**
- IAM Solution Deployment on UNIX Platforms
 - UNIX Integration with IAM
 - System-level IAM Configuration
 - UNIX Security Best Practices in IAM

Training Delivery:

1. **Customized Workshops:**
 - Conduct role-specific workshops tailored to each team's requirements.
2. **Hands-On Labs:**
 - Include hands-on labs to provide practical experience and reinforce theoretical knowledge.
3. **Interactive Sessions:**
 - Foster collaboration through interactive sessions, encouraging questions and discussions.
4. **Documentation:**
 - Provide comprehensive training materials and documentation for future reference.

Conclusion:

This proposed training program is designed to empower each team with the skills and knowledge necessary to excel in their respective roles within the IAM ecosystem. It is our commitment to ensuring a smooth transition, efficient operation, and ongoing success of the Identity Management System at West Virginia Department of Administration.

Team Resumes

Name	NOUMAN ABBASI
Project Role	SENIOR IAM ARCHITECT AND INSTRUCTOR
Years of Experience	17

NOUMAN ABBASI - SENIOR IAM ARCHITECT AND INSTRUCTOR

As a senior IAM architect and instructor, Nouman Abbasi is responsible for designing and implementing robust identity and access management systems within an organization, ensuring secure and efficient access to resources. He develops policies and systems that govern user authentication, authorization, and overall access controls. On the other hand, He is also tasked with educating individuals or groups on IAM concepts, best practices, and technologies. He plays a vital role in transferring knowledge and skills, enabling others to effectively implement and manage IAM solutions. He contributes to maintaining a secure IT environment by designing robust systems and disseminating expertise on identity and access management.

PROFESSIONAL EXPERIENCE

Nouman has served as the Premier IBM Business Partner Security Solution Architect at SPS for nearly 14 years, beginning in 2006 and continuing to the present. With an extensive professional background, he brings over 17 years of experience to his role. Nouman possesses expertise in various technologies and tools, including IAM solutions, QRadar, Guardium, BigFix & MaaS360, ISIPIM, ISIM, MaaS360, Thycotic Secret Server, ITIM, and more

IDENTITY AND ACCESS MANAGEMENT EXPERIENCE:

Asplundh Tree Experts - IAM - IBM ISIM, ISAM, TDI

- Led the team to upgrade ISIM, ISAM, TFIM from 2014 versions to 2018 versions
- Upgraded entire IAM environment of 60,000+ users in less than 6 months, with less than 50 support calls on the cutover day
- Helped Asplundh reduce their helpdesk costs by 70% by implementing a customized ISIM self-service application
- Helped integrate over 12 Cloud services using SAML 2.0, OpenID, and WS Federations
- Integrate 2FA with ISIM self-service application

Asplundh has been a reference customer since 2014

University of Nevada Las Vegas (UNLV) - IBM Security Identity, Access & Single Sign-On

- Architect, Design, and Implement ISIM, ISAM, TFIM & QRadar
- Implement role-based provisioning, de-provisioning, access, single sign-on, and privileged user management
- Upgrade ISIM, ISAM, TFIM to the latest versions (as of 2018)
- Develop and implement Self-Service application using ISIM REST APIs
- Integrate 2FA with ISIM self-service application
- ISIM, ISAM, IGI training for UNLV staff
- Implement IBM Cloud Identity
- Helped integrate over 15 Cloud services using SAML 2.0, OpenID, and WS Federations
- QRadar Deployment, Log Sources Integration & Training

My Eye Doctor - ISPIM, QRadar, Guardium, ISIM, MaaS360, Thycotic Secret Server

- Testing, Configuration, Implementation, LDAP, SIGNA Profiling
- Password Management for SSO - Take VM backups and Snapshots
- Gather the support files before upgrade
- Collect certificates information
- Assemble ISPIM V2.0.1 virtual Appliance upgrade package with existing ISPIM Appliance V2.0.0.0
- Transfer firmware to virtual storage of the installed appliance
- Set the second partition as an active partition
- Format the secondary partition
- Security Identity Management - Validate System Architecture
- Finalize Production Environment
- Privileged Identity Manager - Production Rollout to all users and Internal Walkthrough
- Data Protection using Guardium – Configure and deploy policies and alerts
- QRadar Deployment & Integration
- Managed Security Services including 24x7 Security Operations Center (SOC)

Charmers Sunbelt (CS)

- PIM LDAP and DB2 configs with the appliance
- SessionRecording configs with ISPIM appliance/ DB2 and LDAP config
- SessionRecording configs with ISPIM appliance/ DB2 and LDAP config
- PIM appliance set up for Dev environment - LDAP configs
- PIM pre-configured VM setup

Loudoun County Government, Leesburg, Virginia – ITIM

- Plan, design, architect & lead the team of implementers to deploy IBM ISIM, ISAM ESSO and IBM Privileged Identity Manager at Loudoun County
 - Added IDI data feed on ITIM server to query IDI for an identity feed and tested to ensure communication between ITIM server and IDI
 - Re-imported CSV data into ITIM
 - Integrate 2FA with ISIM self-service application
 - Documented specs for servers

- Created organizational roles, provisioning policies and services in ITIM for various database applications
- Provided analysis of the implementation of background execution of IDI assembly lines
- Created start/stop script to control LDAP tracing
- Installed IBM recommended solution to LDAP hang problem
- Worked on ITIM documentation
- Upgraded ITDI to 6.0 and applied FIX PACK 1 for ITDI 6.0
- Created start/stop script for IDI
- Resolved the Java plug-in issue for ITIM
- Interviewed system administrators to identify provisioning policies
- Provisioned and tested provisioning of users in ITIM and SAP
- Worked on ITIM org tree management
- Authored various scripts for Windows environment
- Lead the team to plan and execute ISIM upgrade with minimum impact to end-users
- Design, architect and implement user self-service application using ISIM REST APIs
- Currently Supporting ISIM operations & expansion

LCVA is a reference customer since 2014.

Time Warner Cable – Louisville, KY

- Design, Plan & Architect ISIM and ISAM implementation

ANAKAM, San Diego, CA – TAM

- Worked on the analysis, requirements, and design of the project.
- ISIM Integration with ANAKAM TFA application (custom adapter) – over 2 million users.
- Led and managed TFA - TAM EAI Adapter Integration
- TFA - TIM Resource Adapter development

HAMILTON BEACH – Glen Allen, VA

- Led and managed single sign-on deployment and training

MARRIOTT, Bethesda, MD – PMR

- Led and managed PMR support and resolution project

CARMAX, Richmond, VA – ITIM

- Worked on the analysis, requirements, and design of the project.
- Led and managed ITIM integration and IMS Upgrade services

Department of Human Services, Hawaii - ITIM, DHS

- Worked on the analysis, requirements, and design of the project.
- Worked with the consultants for the implementation of ITIM and integration with DHS applications.

Maines Paper & Food Service, Inc – Conklin, New York

- Deployment of out-of-the-box Self-Care Application

CareFirst - Owings Mills, Maryland

- Requirements Analysis for FACETS POC
- Assisting the Sr. Consultant in ITIM design for FACETS POC
- Requirements document study for FACETS POC
- Installation & Configuration document preparation

Driscoll Children’s Hospital – Corpus Christi, Texas

- Requirements gathering & design
- Implement Proof of Concept for AD Provisioning Design Document
- Preparing ITIM Express guidelines

Legg Mason, Owings Mills, Maryland – ITIM

- Preparing the Design document for ITIM Implementation
- SPNEGO Integration with TAM
- Part of ITIM, TAM implementation and support team

COURSES / CERTIFICATIONS

Certifications:

- IBM Certified ADP - IBM Service Management Security and Compliance
- IBM Certified Deployment Professional
 - Tivoli Identity Manager V5.1
 - Tivoli Identity Manager V4.6
 - Tivoli Compliance Insight Manager V8.5
 - Tivoli Access Manager for e-business V6.1
 - Tivoli Access Manager for e-business V6.0
 - Tivoli Access Manager for e-business 5.1 Systems Administration
 - Tivoli Access Manager for Enterprise Single Sign-On V8.0.1
- Tivoli Identity Manager Technical Sales Professional (v1)
- IBM Certified Solution Advisor - Tivoli Security and Compliance Management Solutions V3
- IBM Certified Solution Advisor - Tivoli Security and Compliance Management Solutions V2
- Tivoli Security Solution Sales Professional v1
- IBM Certified System Administrator - WebSphere MQ V7.0
- IBM Certified Administrator - Cognos
- IBM Certified BigFix Deployment Professional

Courses:

Following is a list of courses Nouman has taught for SPS.

- Enterprise Identity, Access & Single Sign-On
 - IBM Security Identity Manager
 - IBM Security Access Manager
- Privileged Account Management – Thycotic Secret Server

Name	WADE LEE
Project Role	CUSTOMER SUCCESS MANAGER
Years of Experience	30

WADE LEE - CUSTOMER SUCCESS MANAGER

In his role as a Customer Success Manager, Wade Lee will collaborate with project stakeholders to guarantee overall satisfaction with processes, quality, and the delivery of our solution, ensuring predictable outcomes. His responsibilities include establishing and nurturing the primary business relationship and serving as a seamless interface between the technical team and the project team. Wade will act as the main point of contact for any contract modifications, and as a local resource, he will coordinate and engage in status update meetings. Leveraging his certification as a Design Thinking Engineer, Wade will closely collaborate with the Development and Infrastructure Teams to consistently enhance client satisfaction and return on investment (ROI).

PROFESSIONAL EXPERIENCE

Wade brings over 30 years of experience in the IT arena, encompassing all the key components of client success, including Business Development, Project Management, and Account Management. Actively involved onboarding new customers, understanding clients’ business drivers, building relationships between the client and the support team, and providing a sounding board for future growth. Recognized with the Outstanding Client Service Award for 2018.

CUSTOMER SUCCESS MANAGER EXPERIENCE

Software Productivity Strategists - VP, Partner & Client Success Manager

Asplundh Tree Expert Co

- Meet regularly with CIO of \$4 Billion enterprise
- Track and monitor progress on both Application Development and Cyber Security projects
- Monitor Customer Satisfaction

Altria

- The primary point of contact with the contract manager for \$25 Billion enterprise
- Secured SPS designation on Approved Vendor List
- Coordinated onboarding of SPS Help Desk

LaserShip

- Primary business point of contact for Product Manager
- Participate in weekly calls
- Manage all contractual modifications

REVEL Entertainment

- Implemented and supported IPTV-based technology solutions for 1400 room resort/casino
- Developed, managed, and executed hotel-wide technology installation plan
- Coordinated with Facilities, Entertainment, Guest Services, Marketing, and Construction Union
- Opened the facility on time and within IT Budget
- Supported and trained staff in IPTV Help Desk operations

CERTIFICATIONS & TRAINING

- Certified Scrum Master
- Certified Design Thinking Engineer
- Certified IBM Sales Specialist
- MBA, Marketing, Owen Graduate School of Management, Vanderbilt University
- BA, Economics & Mathematics, Grinnell College

Name	JAMES DEVENPORT
Project Role	PROJECT EXECUTIVE
Years of Experience	30

JAMES DEVENPORT – PROJECT EXECUTIVE

In his role as Project Executive James Devenport provides strategic leadership, oversees project goals and alignment with organizational objectives. He allocates resources effectively, manage risks, and make high-level decisions. He will be responsible for maintaining stakeholder communication, as a Project Executive he will monitor project performance and adjust plans as needed. He fosters a collaborative team environment, engage in client relations, and promote continuous improvement within the project and the organization.

PROJECT EXECUTIVE EXPERIENCE

MorganFranklin Consulting - CIO Advisory Group

- Provide leadership and support for clients.
- Perform IT Assessments for acquisitions and mergers. Lead security assessments for clients followed by developing remediation efforts.
- Provide temporary CISO services and security guidance for organizations as required.

MyEyeDr. Vienna, VA - Chief Information Security Officer

- Developed and implemented a comprehensive security plan for the organization utilizing IBM technologies including QRadar, Guardium, MaaS360, PIM and ISIM.
- Provided a strategic reference for IBM marketing and was involved in beta software review and analysis.
- Published two articles on IBM security projects in the workplace.
- Participated in the IBM X-Force incident response plan. Created plans for 24x7 SOC monitoring of critical infrastructure components.
- Successes include:
 - Security Policy Formulation for a Healthcare Organization
 - Incident Response Plan Including Testing and Remediation
 - Maintain Security and Audit Compliance with PCI and HIPAA Regulations
 - Realtime Dashboard of Current Threats to the Organization

Director of Information Technology

- **IT Department Development:**
 - Established an IT department for a high-growth company in acquisition mode.
 - Led the strategic development and implementation of all IT aspects for the fastest-growing optical company in the country.

- Managed extensive IT integration activities during the organization's rapid expansion.
- **Application Development and Product Management:**
 - Led a cross-functional organization in application development and product management.
 - Managed the integration of subsidiary acquisitions and strengthened security for compliance.
 - Developed budgets, obtained funding, and improved overall technology functions.
 - IT Infrastructure Expansion and Restructuring:
 - Established an IT infrastructure for a fast-growing organization.
 - Restructured the IT department, growing from two technicians to a team of 27.
 - Implemented a hierarchy of managers and specialized teams for various IT functions.
- **New Intranet and Reporting Portal:**
 - Designed and implemented an intranet with unit-specific sharing spaces.
 - Instituted a reporting strategy for divisions and offices, enhancing deficiency correction.
 - Implemented a login system for managers to review specific reports, promoting faster action.
- **Cloud Migration:**
 - Planned and supervised the migration of critical infrastructure to the Cloud.
 - Addressed the need for greater storage and uniformity among offices.
- **Telecommunications Strategy:**
 - Updated telecommunications systems to accommodate rapid growth.
 - Managed procurement processes, from RFP creation to vendor selection and implementation.
- **Privacy and Security:**
 - Planned, developed, and implemented a multi-layered data security strategy.
 - Established an emergency response plan for data theft, breaches, and ransomware.
 - Created a training plan to help employees recognize and respond to phishing attempts.
- **Disaster Recovery:**
 - Launched a disaster recovery plan, spreading critical data among multiple data centers.
 - Moved legacy data to a cloud environment for improved security and remote support.
- **Revitalized Website:**
 - Developed and launched a new website in collaboration with the marketing department.
 - Highlighted new corporate branding and streamlined the appointment process with a new patient portal.
- **Call Center Creation:**
 - Oversaw the development of a functional call center with a real-time dashboard.
 - Implemented a system to track staff effectiveness in answering calls and created uniform reporting across the organization.

The Washington Post - Senior System Administrator

- Responsible for legacy Lotus Notes/Domino Infrastructure.
- Analysis of existing applications and determining needs and feasibility for application conversion.
- Conversion of Lotus Notes applications to SharePoint for Microsoft Office 365 Cloud implementation.
- Migration of Lotus Notes Mail files, Lotus Notes Archive files and Exchange to Microsoft Exchange in the Cloud.

AvalonBay Communities, Inc. - Senior IT Manager / Web & Application Development

- Directed key IT functions for a \$10 Billion Fortune 500 Company.

- Collaborated with senior management and others to identify requirements, develop plans, and budgets.
- Guided projects to completion, ensuring alignment with organizational goals.
- Managed licensing and compliance requirements for numerous applications and systems.
- Oversaw usage and applications for Blackberry, Android, and Apple products.
- Led eDiscovery initiative to provide support for litigation requests.

Certifications

- C|CISO Certified Chief Information Security Officer
- Issued by EC-Council, Certificate Number [REDACTED] Valid 3/2/2018 – 3/1/2021
- IBM Certified Application Developer, Lotus Notes and Domino 7
- IBM Certified Advanced Application Developer, Lotus Notes and Domino 7

Name	VIREA BAYLOR
Project Role	PROJECT MAMAGER
Years of Experience	7

VIREA BAYLOR – PROJECT MANAGER

Accomplished administrative professional with a robust history of overseeing projects, and teams, ensuring operational excellence. Demonstrated proficiency in delivering diverse technical services and support within Information Technology (IT) through staff augmentation and project-based consulting. Expertise extends to recruitment, procurement, and organizational management. Adept in coordinating schedules, streamlining office operations, and ensuring outstanding client service. Committed to enhancing organizational success through administrative excellence.

PROFESSIONAL EXPERIENCE

With a seasoned background in project management, she brings a wealth of experience to the table. Her expertise lies in effectively leading teams, managing project scope, and ensuring successful project outcomes within specified timelines and budgets. Known for her adept communication with stakeholders, she has a proven track record of driving quality assurance and continuous improvement initiatives.

Software Productivity Strategists - Business Operations Assistant/Project Management

- Provide comprehensive administrative support to the business operations team, including managing calendars, scheduling meetings, and handling correspondence.
- Developed comprehensive project plans outlining timelines, milestones and deliverables.
- Executed project plans, ensuring adherence to deadlines and budget constrains
- Maintaining and updating databases, spreadsheets, and records to ensure accurate and organized data for business operations.
- Create, format, and manage business documents, reports, and presentations, ensuring professionalism and accuracy.
- Identify and recommend process improvements to enhance efficiency in business operations, streamline workflows, and reduce operational costs.
- Manage office supplies, inventory, and procurement, ensuring that necessary resources are readily available.
- Assist with financial tasks such as tracking corporate spending, expense reporting, and invoice processing to support financial management and reporting.
- Coordinate meetings, including scheduling, preparing agendas, and organizing necessary materials. May also take minutes and follow up on action items.
- Serve as a point of contact for internal and external inquiries, ensuring effective and professional communication.
- Record Keeping: Maintain organized and accessible records of business operations activities, contracts, and agreements.
- Project Assistance: Support various business projects by assisting in research, data analysis, and project coordination tasks.

- Provide support to customers or clients by addressing inquiries, resolving issues, and ensuring a high level of customer satisfaction.
- Assist in ensuring that the business operations adhere to relevant laws, regulations, and compliance requirements.
- Assist with the setup and troubleshooting of technical equipment and software used in business operations.
- Reporting: Generate and distribute regular reports to provide insights and updates on business operations to relevant stakeholders.
- Liaise with vendors, contractors, and service providers, managing relationships and contracts as needed.
- Assist in training and onboarding new employees to familiarize them with business processes and procedures.
- Monitor and maintain the quality and consistency of operations, addressing any deviations from established standards.
- Conduct research on industry trends, competitors, and best practices to inform business strategy.

Reaction Retail (TEMP AGENCY) - Rockville, MD - Account/Office Manager

- Managed contracts and projects of similar size, overseeing office area and warehouse.
- Coordinated schedules, bookings, and appointments, demonstrating the ability to provide the breadth of technical services required under the contract.
- Conducted product/market research, file management, and organized orientation and training of new staff, aligning with IT staff augmentation and project-based consulting services.
- Oversaw office supply acquisitions and acquired knowledge of billing/collection practices.
- Curating spreadsheets and PowerPoints for clients (Bloomingdale's, Macy's, Ulta) and scheduled freight deliveries to two offices (Maryland & California).
- Demonstrated expertise in recruitment methods for information technology-related services and support.

Arbee Associates (TEMP AGENCY) - Gaithersburg, MD - Front Office Manager/Administrative Assistant

- Managed databases and organized warehouse pick-up, aligning with company events and conferences.
- Ordered stationery and furniture, demonstrating proficiency in procurement.
- Prepared letters and reports, managed office budgets, and maintained office administrative systems, aligning with managing contracts and maintaining procedures.
- Answered phones, scheduled appointments, and maintained calendars, handling correspondence and complaints.
- Created and maintained filing systems, both electronic and physical.
- Liaised with staff, suppliers, and clients, ensuring health and safety policies were up to date.

Payroll Specialist - KDB (TEMP AGENCY) - Rockville, MD

- Processed payroll, maintained the employee database, and reported to the department supervisor regarding daily activities and issues, showing strong knowledge of fiscal procedures.
- Managed the company budget and expenses, collaborated with different departments, and addressed employee complaints related to the payroll system.
- Fulfilled all aspects of payroll, including time preparation, entry, processing, and check printing.
- Managed accounts and performed bookkeeping, demonstrating expertise in payroll services.

- Conducted bank reconciliation and other accounting and administrative functions.

Administrative Assistants - The Baylor Company - Potomac, MD

- Consulted with representatives of regulatory agencies to complete accurate filings and uphold strict compliance, aligning with regulatory requirements in contract management.
- Improved overall financial reporting and financial control processes.
- Attended monthly sales meetings and reported pertinent information to employees, enhancing collaboration with senior leadership.
- Developed loyal customer relationships through proactive management of client service strategies.
- Established and optimized schedules to align with forecasted demands and exceeded sales goals.

Administrative Assistant/Client Services - Visioneerit - Baltimore, MD

- Used Excel and Adobe to create presentations, reports, and spreadsheets, showcasing proficiency in technical support.
- Managed executive calendars and answered multiple console telephone system calls, highlighting administrative support skills.
- Monitored office supplies and kept physical and digitized records organized.
- Managed supervisor itinerary and appointments, tracked and recorded expenses, and enhanced collaboration between team members.

Business Consultant - Shaun Auto Sales - Baltimore, MD

- Devised, deployed, and monitored processes to boost business success, aligning with strategic management.
- Conferred with customer account representatives to service accounts, enhancing client satisfaction and providing business consulting.
- Provided primary customer support to internal and external customers, promoting repeat business.
- Cultivated customer loyalty and improved sales through personalized business consulting.

Assistant Store Manager - Koi Tea - Stafford, VA

- Managed opening and closing procedures and coached sales associates, significantly increasing customer satisfaction.
- Applied performance data to evaluate and improve operations, forecast needs, and enhance staff management.
- Conducted weekly staff meetings to motivate team members, address concerns, and evaluate progress toward goals.

COURSES / CERTIFICATIONS

Certifications:

- Certified Payroll Professional

Name	MARY STANG
Project Role	CONTRACTS MANAGER
Years of Experience	27

MARY STANG – CONTRACTS MANAGER

A dedicated and results-oriented Contracts Manager with 27 years of experience in managing contracts across Higher Education, State, Local, Federal, and Commercial sectors.

PROFESSIONAL EXPERIENCE

Software Productivity Strategists - Director – State, Local, Education

- Manage and oversee four contracts for the State of Maryland involving Hardware, Software, and Services, and Commonwealth of Virginia (VITA IBM Software and Services) ensuring compliance and successful revenue outcomes.
- Responsible for analyzing daily receipt of PORFPs using internal Business Management System (BMS) and tracking revenue successes.
- Identify and pursue additional opportunities, leading and supporting responses for RFPs in State and Local jurisdictions.

Alliances and Partnerships Manager

- Work with Management to identify key partner relationships with tech providers, distributors, and other resellers.
- Once identified, work through the application process including agreements that need to be approved through our legal process.
- Meet with channel managers to review the partnership relationship and set up sales, technical and marketing training so goals of success can be set
- Manage the Partner portals along with access for team members at SPS.

Contracts Manager

- Managed contract relationships with all customers, resellers, distributors
- Reviewed and kept current internal SPS professional services, schedules, master subcontract agreements and exhibits with upper management
- Prepared the appropriate contract to be provided to the various entities that we worked with.
- Responded to and SPS was awarded four State of Maryland contracts:
 - Desktop, Laptop and Tablet 2015 Master Contract
 - Commercial Off-the-Shelf Software (COTS 2012)

- Consulting and Technical Services+ (CATS+)
- Hardware 2012 Master Contract
- Provided support and review during the Federal GSA process
- Worked with upper management on Federal SBA 8(a) paperwork
- Managed our relationship with our insurance broker to make sure that our insurance met the requirements of the contracts and RFPs we responded to.

AITP Manager

- Managed the IBM Authorized Independent Training Provider program.
 - Coordinated all aspects of classes such as:
 - Sourcing instructors internally for from outside sources
 - Course materials provision, schedule of classes, post to websites, co-ordinate instructors and student's needs, imaging and setting up equipment for classes. Setting up processes for smooth class sessions

Name	RAINER L. BARTHEL
Project Role	SECURITY ARCHITECT
Years of Experience	14

RAINER L. BARTHEL - SECURITY ARCHITECT

Accomplished Security Architect with 14 years of experience, focused on delivering tangible results. A seasoned technical expert, with over 25 years in Security Sales, Business Development, and Management, driving positive outcomes and boosting the success and financial gains of multimillion-dollar enterprises. A charismatic leader known for exceptional organizational prowess, renowned for kickstarting and nurturing startup initiatives, as well as driving the expansion of businesses spanning the U.S. and Europe. Showcases both proven technical acumen and sales proficiency, with a demonstrated ability to foster, oversee, and fortify client relationships. A skilled communicator adept at steering international projects, consistently surpassing corporate objectives.

SOFTWARE PRODUCTIVITY STRATEGISTS, Rockville, MD - Security Management as a Service September

- Spearheading the Security Management Department, delivering security consulting, assessments, and managed security services.
- Cultivating robust connections with key figures in the technology market and IBM globally.
- Marketing and selling security solutions and services to clients on a global scale.

MAINLINE INFORMATION SYSTEMS, Tallahassee, FL - Security Architect May

- Leveraging security architecture expertise to assist the Mainline Sales Organization across the United States and Puerto Rico in the full spectrum of Security and Business Continuity/Disaster Recovery service and product offerings. Converting business requirements into effective security solutions while upholding relationships with clients, vendors and partners.

INTIGROW, Duluth, GA - Senior Sales Executive Public Sector and Commercial Accounts

- Build the Public Sector Practice
- Initiated and managed new accounts including Maryland Benefit Health Exchange and Missouri Medicaid
- Reinitiated strong relationships to key manufacturers within the technology market including IBM worldwide

**SOFTWARE PRODUCTIVITY STRATEGISTS, Rockville, MD - VP of Security Solutions & Business Analytics
May**

- Built the Security Solutions Division (IBM: IAM, QRadar, Tivoli, Lotus, WebSphere, Cognos - SourceFire, RSA) with Sales exceeding 2.5 million
- Built strong relationships to key players within the technology market and IBM worldwide
- Lead Technical Security Team with over 20 engineers

EASTBANC TECHNOLOGIES, Washington, DC - Director of Business Development July

- Initiated and managed new accounts including Citibank with revenue of >\$1million
- Built strong relationships to key players in the technology mark

ACTIVE NETWORK SYSTEMS, Hamburg, GER - President & CEO/Part Owner

- Established and managed day-to-day operations including sales, account development, business planning, partner relationships, and customer service. Recruited, trained, and supervised staff of 28 including sales representatives, technicians, and administrative personnel.
- Developed more than 1000 customer accounts, resulting in annual revenues exceeding \$15 million
- Forged profitable relationships with key companies including Hewlett-Packard, IBM, Dell, Fujitsu-Siemens, Cisco, Avaya, Extreme Networks, McAfee, Microsoft etc.
- Won lucrative defense account, formerly served by HP, resulting in revenue of \$1.5 million annually.
- Established and supervised U.K. subsidiary.
- Named 1 of Top 10 HP resellers in Germany
- Largest single deal \$ 1.5 million (Extreme Networks installed on German warships)
- Founded Internet-based company, specializing in international trading platforms.

KELLY COMPUTER SYSTEMS, Hamburg, Germany - Managing Director European Operations January

- Established and guided the initiation of new ventures in Germany, the United Kingdom, and Finland. Orchestrated the operational launch, overseeing sales activities and fostering connections with system manufacturers. Enlisted and nurtured a 15-member team encompassing sales representatives, technicians, and administrators. Assumed responsibility for all legal and administrative aspects concerning the establishment of European-based subsidiaries. Conducted comprehensive research to build a customer database and formulated supplier contracts. Orchestrated the execution of marketing initiatives, encompassing global mailings and participation in trade exhibitions.
- Attained profitability for European operations within a swift 3-month period from inception.

- Secured backing from Hewlett-Packard for Kelly 3rd party memory across the UK & EU
- Formulated an expansive reseller network in the EMEA region, resulting in revenue growth from zero to \$5 million.
- Enhanced profitability by adeptly identifying and forging partnerships with cost-efficient suppliers.

OPERATIONS CONTROL SYSTEMS, INC., Palo Alto, CA - Project Director European Market April

- Managed introduction of OCS products into European market. Created and maintained accounts with customers in France, Germany, and the Benelux.
- Spearheaded presence in European market, setting up reseller network in several countries and establishing accounts with key customers.
- Managed accounts with revenue in excess of \$1 million.
- Pursued and closed \$250,000 software deal with Compaq Munich

HI-COMP AMERICA, INC., New York City, NY - President

- Oversaw U.S. operation of German-based company. Managed major client accounts including Hewlett-Packard, State Farm Insurance, McDonnell Douglas, Owens Corning and Pillsbury.
- Grew annual sales revenue from less than \$100,000 to more than \$1 million.

Schneider Versandhandel Hamburg, GER (Mail-Order/Retail Company) – Chief Information Officer

Coutinho Caro & Co Hamburg GER (Steel Trading/International Constructing) - Chief Information Officer

CERTIFICATES

- IBM Champion 2022 & 2023
- IBM Security Sales/Technical Certificates complete IBM Security Portfolio
- IBM Cloud Pack for Security Palo Alto Network System Engineer (PSE)
- Palo Alto Network Prisma, PAN-OS, Cortex Proofpoint Various Sales Certificates Arctic Wolf Various Sales Certificates
- CrowdStrike Various Sales & Technical Certificates ZScaler Various Sales & Technical Certificates Imperva Various Sales & Technical Certificates Ivanti Various Sales & Technical Certificates
- Mist Various Sales & Technical Certificates
- Okta Various Sales & Technical Certificates
- Centrify (Delinea) Various Sales & Technical Certificates

Name	MANOJ SHRESTHA
Project Role	IAM SUBJECT MATTER EXPERT
Years of Experience	21

MANOJ SHRESTHA – IAM SUBJECT MATTER EXPERT

With nearly nineteen years of experience, Manoj is a seasoned consultant specializing in IBM Certified Identity and Access Manager and WebSphere technologies. His expertise spans the entire project lifecycle, encompassing planning, design, installation, configuration, testing, training, and support of intricate IAM and WebSphere deployments in high-availability enterprise environments. Manoj excels in gathering and documenting functional requirements, designing technical architectures and processes, and implementing various IAM product components, including upgrading versions of ISIM, ISAM, TFIM, QRadar, and the overall IAM environment. Notably, he has successfully implemented customized ISIM self-service applications, facilitated the integration of cloud services, managed deployment processes, integrated log sources, and conducted comprehensive training sessions.

PROFESSIONAL EXPERIENCE

A seasoned consultant specializing in IAM and WebSphere, providing expertise to clients for the design and deployment of IBM WebSphere, IBM Security Identity Manager, IBM Security Access Manager, and Security Federated Identity Manager

Asplundh Tree Experts - IAM - IBM ISIM, ISAM, TDI

- Led the team to upgrade ISIM, ISAM, TFIM from 2014 versions to 2018 versions
- Upgraded entire IAM environment of 60,000+ users in less than 6 months, with less than 50 support calls on the cutover day
- Helped Asplundh reduce their helpdesk costs by 70% by implementing a customized ISIM self-service application
- Helped integrate over 12 Cloud services using SAML 2.0, OpenID, and WS Federations
- Integrate 2FA with ISIM self-service application
- Asplundh has been a reference customer since 2014

University of Nevada Las Vegas (UNLV) - IBM Security Identity, Access & Single Sign-On

- Architect, Design, and Implement ISIM, ISAM, TFIM & QRadar

- Implement role-based provisioning, de-provisioning, access, single sign-on, and privileged user management
- Upgrade ISIM, ISAM, TFIM to the latest versions (as of 2018)
- Develop and implement Self-Service application using ISIM REST APIs
- Integrate 2FA with ISIM self-service application
- ISIM, ISAM, IGI training for UNLV staff
- Implement IBM Cloud Identity
- Helped integrate over 15 Cloud services using SAML 2.0, OpenID, and WS Federations
- QRadar Deployment, Log Sources Integration & Training

Loudoun County Government, Leesburg, Virginia – ITIM

- Plan, design, architect & lead the team of implementers to deploy IBM ISIM, ISAM ESSO, and IBM Privileged Identity Manager at Loudoun County
 - Added IDI data feed on ITIM server to query IDI for an identity feed and tested to ensure communication between ITIM server and IDI
 - Re-imported CSV data into ITIM
 - Integrate 2FA with ISIM self-service application
 - Documented specs for servers
 - Created organizational roles, provisioning policies and services in ITIM for various database applications
 - Provided analysis of the implementation of background execution of IDI assembly lines
 - Created start/stop script to control LDAP tracing
 - Installed IBM recommended solution to LDAP hang problem
 - Worked on ITIM documentation
 - Upgraded ITDI to 6.0 and applied FIX PACK 1 for ITDI 6.0

Virginia State Police (VSP)

- Migrated IBM Tivoli Access Manager environment from ITAM v6.1.1 to Security Access Manager V9.0.4
- Migrated IBM Tivoli Federated Identity Manager v6.1.1 to ISAM v9.0.4 – Federation Module with Advanced Access Control
 - User Self-Care setup
 - Migrated over 12+ FIM partners

Time Warner Cable – Louisville, KY - Senior TIM/TAM/TFIM + WebSphere Consultant

- Provided Unified single sign-on to Insight Webservices
- TFIM deployment fro Federated Identity to HBO, CINEMAX, and NBC Olympics

EQUIFAX (ANAKAM) – San Diego, CA - Senior WebSphere and TIM/TAM Developer

1. TFA - TAM EAI Adapter Integration
2. TFA - TIM Resource Adapter development

MARRIOTT – BETHESDA, MD - Senior TIM/TAM/WebSphere Consultant

- PMR support and resolution

HAMILTON BEACH – Glen Allen, VA - Tivoli Consultant

- TAM-ESSO deployment and training

CARMAX – RICHMOND, VA - Senior WebSphere and TIM/TAM Consultant

- Worked on ITIM integration and IMS Upgrade services

DRISCOLL CHILDREN'S HOSPITAL - TAM-ESSO Consultant

- Built clustered production environment.
- Set-up test environment
- Installed the IMS server and components of TAMESSO. Set-up load balancer on 2 nodes.
- Worked on Profile enhancement.
- Configured EPIC profile.
- Configured Lawson Employee Portal Profile (WebApp)
- Configured GE PACs Profile (WebApp)
- Configured multi-factor RFID authentication.
- Configured user self-service (reset/ & change PWD)
- Created TAMESSO documentation.

DEPARTMENT OF HUMAN SERVICES – HAWAII - Senior WebSphere and TIM/TAM Consultant

- Completed the installation checklist for the installation of TAMESSO, TAMEb, and TIM.
- Installed TAMEb Policy Server, TAMEb WebSeal Server, and Tivoli Identity Manager Server
- Installed the IMS server and components of TAMESSO.
- Configured TAMEb Junction and tested ACL with webserver.
- Installed and configured TAMEb Combo Adapter
- Configured application profiles for Single-Sign-On to WebApps (IBM Host on Demand, Portal), Client-Server based (Lotus Notes), and Mainframe systems (HAWI).
- Installed and configured TAMESSO Adapter
- Configured TIM to work and integrate the provisioning process with TAMESSO.
- Delivered the TAMEb training session to the DHS team.
- Deliver TAMESSO training sessions to the DHS team.
- Created TAMEb training manuals.

- Installed and Deployed Pilot Solution with
 - WebSphere
 - TAMESSO
 - TAMeb
 - TIM

ERIE 1 BOCES – ERIE, NEW YORK - OmniFind Senior Consultant

- Worked on VPN Access, verification, and discovery.
- Setup OmniFind Search in Portal Server.
- Configured Portal for OmniFind
- Setup, configured and tested WebSphere Portal crawler
- Troubleshoot, configured, and tested WCM Crawler
- Configured DB2 crawler
- Configured Notes crawler.
- Tested and communicated on DIOP and NRPC.
- Configured security for OmniFind.
- Provided documentation on Securing OmniFind and Configuring Portal Crawler.

SUNGARD ASSET MANAGEMENT SYSTEMS, LLC - MALVERN, PENNSYLVANIA - Sr. WebSphere Portal Server and TAM Consultant

- Worked on troubleshooting DataSource Oracle
- Worked on troubleshooting LTPA issue
- Investigated JavaCore/AJAX
- Installed AJAX application and configured website
- Worked on troubleshooting AJAX issue
- Worked on performance tuning (PMI and Logging) and FTPing the files

MAINES PAPER & FOOD SERVICE – CONKLIN, NEW YORK - Sr. WebSphere Portal Server and TAM Consultant

- Integration of WPS with TAM
- SSO between WPS and TAM WebSEAL using LTPA token
- Designed and Implemented DIT for enterprise directory
- SSO with Domino components with Portal
- SSO with Cognos and Desktop SSO

ERIE 1 BOCES – ERIE, NEW YORK - Sr. WebSphere Portal Server and TAM Consultant

- Integration of WPS with TAM
- SSO between WPS and TAM WebSEAL using TAI++
- Design and implementation of DIT
- Worked on Log-off options for WPS portal

- Created and configured Virtual Host Junction for Websphere portal.

LEGG MASON – OWINGS MILLS, MARYLAND - Sr. WebSphere Portal Server and TAM Consultant

- Install and configure Tivoli Access Manager
- Install and configure Tivoli Identity Manager in a clustered environment
- Externalize security both Authentication and Authorization for WAS applications
- Assisted in self-care and self-registration module of TIM

PUBLISHERS PRINTING COMPANY - SHEPHERDSVILLE, KENTUCKY - Sr. WebSphere Portal Server and TAM Consultant

- Created Provisioning, password and identify policies to the provision to Tivoli Access Manager for e-business and WebSphere Portal server
- Analyzed user registry data structures to synchronize source and destination data mapping
- Customized java server pages for the registration forms to include unique subscriber attributes
- Customized Registration Servlet to automate the subscriber self-registration and email notification process
- Tested and documented the self-registration application
- Worked on debugging TIM to resolve the reconciliation and association issue between TIM and TAM.

COURSES / CERTIFICATIONS

Certifications:

- IBM Certified Advanced Systems Administrator
- IBM Certified Systems Expert Administration
- IBM Certified Instructor for WebSphere Application Server (multiple)
- IBM Certified WebSphere Application Server Network Deployment (multiple)
- IBM WebSphere MQ V7.0 System Administration Application Server (multiple)
- IBM Certified TIM/TAM/TAM-ESSO/TFIM (multiple)

Courses / Professional Trainings

- IBM Tivoli Access Manager System Administration
- IBM Tivoli Identity Manager Administration
- IBM Federated Identity Manager – Single sign-on
- Linux System Administration
- Citrix NetScaler System Administration

Name	IMRAN MUFTI
Project Role	IAM SUBJECT MATTER EXPERT AND INSTRUCTOR
Years of Experience	25

IMRAN MUFTI – IAM SUBJECT MATTER EXPERT AND INSTRUCTOR

In his role as an IAM Subject Matter Expert (SME), Imran Mufti has played a crucial role, utilizing his profound expertise in identity and access management to offer strategic guidance and address intricate challenges in security practices. Functioning as a consultant, he ensures that organizations effectively design, implement, and optimize IAM solutions. Simultaneously, in his capacity as an IAM Instructor, Imran contributes to knowledge dissemination by educating individuals on IAM concepts, tools, and best practices. Through curriculum development, facilitating learning experiences, and promoting skill transfer, he empowers others to comprehend and proficiently implement IAM solutions in practical scenarios, thereby elevating overall organizational security and compliance.

PROFESSIONAL EXPERIENCE

With over twenty-five years of professional experience, the last two decades of which have been dedicated to Cybersecurity and related domains such as Database Security and Monitoring, Identity and Access Management, and Security Information and Event Management (SIEM), Imran has acquired extensive expertise in IBM suite products (Guardium, ISIM, ISAM, QRadar, TDI/IDI), along with proficiency in SNMP-based network monitoring tools. Imran has served as both an Instructor and consultant at SPS since 1997, bringing his wealth of knowledge to the organization. Considering his overall experience, he boasts a comprehensive background spanning various technologies and tools within the realm of Cybersecurity.

Ottawa Hospital, Teknor, Planco, Univ. of Maryland University College, Phillips Electronics Netherlands, Federal Reserve Bank, Patent and Trademark Office

- Installed and configured Tivoli Identity Manager 4.5. This required installation of LDAP, DB2, WebSphere, and Identity Manager Servers on Windows 2000 and NT Agents. Set up a DSML feed and imported user-data from SAP HR system and user-account information from the Windows NT 4 Domain environment into TIM. Configured user self-service for password management.
- Configured and deployed a distributed Network Management System based on HP OpenView Network Node Manager, consisting of five collection stations and two management stations for redundancy, ten management consoles with management domain spread over all of the US. Prepared an “as-built” document in support of the project.
- On-call in NOC for resolution of complex problems, as well as trained the operators and supervisors in day to day operations
- Installed, customized maps, defined filters, configured alarms

- Integrated with other third-party products as CiscoWorks, Paradyne (CSU/DSU) OpenLane, and Cylink Privacy Manager
- High-level presentation/training on Network Management System, to management/employees of the client
- Tested the system in test-lab, set up at Federal Reserve
- Assisted in the deployment of PAIR application using HP-Virtual Vault, a B-1 certified, secure web front end for applications.
- Configured and tested the Raptor firewall.
- Provided support at the client end to complete the Oracle-Forms project; troubleshooting, testing, documentation, and WinFax-Pro server support.
- Hosted and maintained a website for various projects
- Wrote the website maintenance manual, which was greatly appreciated by the client.
- Hosted website for ACPS, to act as a central information point for all. Progress tracked using MS-Project and posted on this website. He also mirrored this website on the local ACPS server.
- Administered PC Networks based on NT domain.

U.S. Department of Homeland Security -mCustoms and Border Protection - IBM Security Identity and Access Manager Consultant

- Managed IBM Tivoli Identity and Access Manager deployments at DHS.
- Developed workflows for the handling of user management for a new class of users. Automatically assigned "Roles" based on location/container a user is created in, including scripting to deal with creation, transfers, and de-activation
- Developed script to resolve password synchronization anomalies between ITIM and SAP back-end systems, for different roles.
- Developed provisioning policies for SAP back-end systems including mapping of roles
- Solved production issues by troubleshooting various components of identity and access management software
- Researched and prepared a preliminary design for synchronization of LDAP attributes between Mainframes
- Provided L3 support for user provisioning issues in the Production system
- Worked on Bulk Upload of User data, using IBM Directory Integrator. Documented the process
- Developed system for duplication of ITIM environment using LDIF files and ITIM Import Export Facility and made this a CM controllable process.
- Investigated Entrust-Truepass solution for digitally signed and secure web-based transactions; setup lab systems Certificate Authority, Truepass, and IBM-WebSphere Portal for testing
- Prepared User data for loading in the production system – from legacy to new release of ACE, including data mapping and clean up
- Supported customized code which brokers password expiry and changes between front end and user provisioning system
- Researched, tested, and documented security policy-based execution of digitally signed Java applets for deployment on Govt. Workstations; involves writing policy files and managing digital certificates using Java security tools
- Worked with the System Integration Test team in efforts for planning and writing tests for the new release

Virginia State Police - ISAM Consultant

- Upgraded Policy Server, and Reverse Proxies from version 6.x to version 9.x (appliances) in three environments
- Upgraded IBM Directory Servers from v.6.x to v.8.x (appliance), building six LDAP servers from the ground up and transferring current data
- Upgraded IBM Security Directory Integrator, transferring current assembly lines to the new environment
- Upgraded User-Self Care module of Tivoli Federated Identity Manager
- Worked on migration of User-Self-Care to ISAM SCIM in Advanced Access Control, from Tivoli Federated Identity Manager
- Developed procedure to move and verify LDAP data from the current production environment to a new environment.

US- Dept. of Justice, Cybersecurity Services, Guardium (Data Security) Consultant

- Coordination with component agencies for Deployment, Configuration, and Reporting
- Developed Workflows for Deployment, Interaction between Agencies and CyberSecurity Services
- Configured Security/Vulnerability Assessments Scanning and Reports
- Developed Baseline Policies (Security Rules) for DAM (Data Access Monitoring)
- Configured and Scheduled Reports on database usage for component agencies
- Modified Base Policies and Groups after some data was collected
- Installed GIM and STAP on database servers
- Configured Data Level Access Control (so that one Agency cannot view another Agency's data)
- Configured STAP > Collector Load Balancing
- Data transmission to SPLUNK

MyEyeDr, Guardium and QRadar Deployment Consultant

- Upgraded Guardium 9.x to 10.x
- Installed GIM and STAP on database servers
- Integrated events generated in Guardium with QRadar, which serves as a single-window into IT activities, giving a holistic picture
- Developed Guardium Policies/Rules to filter through database activities, using trusted access/connection profiles and user groups to identify any untrusted access.
- Classified and deployed rules to curtail "noise" in observed transactions, the record for audit, and send alert where necessary.
- Integrated Guardium Login and Guardium Groups with Active Directory
- Developed and scheduled daily, weekly, and monthly reports, listing violations to rules, new connection profiles, and vulnerability assessments.
- Evaluated compliance with PCI standards.

- Oversaw solution architecture considering network topology and client objectives
- Defined Network Hierarchy for Internal network and DMZ, which included cloud environment
- Configured Log Sources, including general Windows, DNS and database servers
- Configured Flow Sources to collect network activity from networking devices
- Customized dashboards
- Currently working on identifying false positives and fine-tuning rules with the intent of early warning of malicious activities.

Various Clients, (Maryland Insurance, Virginia Commonwealth Univ, Loyola Univ), QRadar Deployment Consultant

- Installed and base-configured
- Upgraded QRadar in an existing environment; upgrade document delivered
- Configured Log Sources, including general Windows (using WinCollect), DNS and database servers as well as Firewalls and Linux Servers
- The configured Vulnerability Assessment tool

Imparted training on the use of QRadar

COURSES / CERTIFICATIONS

Certifications:

- IBM Security Guardium 10 & 9 Technical Training (IBM Certified in Guardium)
- IBM Tivoli Access Manager 4.1 System Administration & Planning (IBM Certified in Access Manager)
- HP Network Node Manager I on Unix (HP Certified)
- HP OpenView ManageX (HP-Certified)
- HP OpenView DeskTop Administrator (HP Certified)

Courses:

- IBM BigFix Content Development
- IBM Security QRadar 7.2 Administration and Configuration
- IBM Security QRadar SIEM Foundations
- IBM Security Federated Identity Manager 6.2.2 Deployment and Administration
- IBM Security Identity Manager 6.0 Basic Administration
- IBM Tivoli Identity Manager 4.4 & 4.5 Planning, Installation, Administration and Configuration
- IBM SecureWay Vault Registry for PKI – Planning, and Implementation
- IBM Tivoli PKI (SecureWay Trust Authority) Fundamentals
- IBM Tivoli PKI (SecureWay Trust Authority) Planning & Implementing
- AIX, Solaris, Linux, Network and System Administration courses
- HP Network Node Manager I on NT
- HP Network Node Manager for operators

Name	RIZWAN ALI
Project Role	IAM SUBJECT MATTER EXPERT
Years of Experience	10

RIZWAN ALI – IAM SUBJECT MATTER EXPERT

With almost a decade of professional experience, Rizwan is a highly skilled consultant with a focus on IBM Certified Identity and Access Manager and WebSphere technologies. His proficiency extends across the entire project lifecycle, covering planning, design, installation, configuration, testing, training, and support of complex IAM and WebSphere deployments within high-availability enterprise environments. Rizwan excels in tasks such as gathering and documenting functional requirements, designing technical architectures and processes, and implementing various IAM product components.

PROFESSIONAL SUMMARY

Rizwan has been working with SPS 2010 to present as a IAM SME, with over 10 years of vast experience Rizwan had done his hands dirty on diverse technologies in the field of Security and has been engaged in assisting customers plan, design, and implementation of Security services. He has expertise in IBM Security QRadar, IBM BigFix, MaaS360 Tivoli Storage Manager, IBM Security, and Guardium.

Asplundh

1. QRadar – Installation Team Enablement, Initial Tuning, Advanced Tuning
2. Data Classification

Carilion Services, Inc

- Delivered customized 10 days of training on both IBM MaaS360 and IBM QRadar

Health Resources and Services Administration (HRSA)

Helped to develop and deliver the following classes:

1. IBM BigFix Platform Foundations (IS720G)
2. IBM BigFix Content Development (IS730G)
3. Custom IBM IBM BigFix Lifecycle, Inventory, Compliance, and Patching classes

MetaCoastal

- Set up POC
- Reinstallation of BigFix
- Implementation
- Knowledge transfer

Lasership

- QRadar – Installation Team Enablement, Initial Tuning, Advanced Tuning

My Eye Dr

- Guardium – Installation, and Configuration
- QRadar – Installation Team Enablement, Initial Tuning, Advanced Tuning

The University of Nevada, Las Vegas Nevada

- Support and Maintenance
- IAM Implementation
 - Installation of TDS and DB2
 - Installation of SAM for Web
 - Installation of website and policy server

Artesian Water Works

- Did Assessment for QRadar
- Upgraded QRadar to the latest version
- Implemented new rules.
- Created new Alerts

Department of State Correctional Services, State of Maryland

- TSM – Upgrade Server and Nodes

NetOptics

- Developed Spyke course for NetOptics, assisted in creating & documenting of Runbooks

Solutions-II

- Created role-based Runbooks

Good Samaritan, US

- TAM ESSO Training

Insight Communications – Louisville, KY

- TSRM Help Desk Implementation

First Bank of Puerto Rico

- ITIM Documentation

Cybersecurity Support Specialist

- Understand Cyber Security requirements and propose solution options
- Deployed SIEM Solution at four different clients and provided Knowledge transfer.
- Installation, Configuration, Customization, Support and Training of security products and solutions
- Design and Architect Security solutions.
- Customize and Extend Security products to map into customer requirements
- Conduct assessments and recommend tools and services

Asplundh

- Performed the Complete Requirement Gathering for the Client.
- Provided the definition, planning, and implementation of QRadar.
- Provided the documentation of AS-IS and TO-Be phases as well as the success criteria for the

project completion.

- Identified the Assets of the organization for the gathering of logs and Flows.
- Performed Data Classification for the Client to access the auditing requirements.
- Worked on the PII requirements for the client and helped with HIPPA compliance.
- Created a process of Mapping said assets to Asset owners for proper escalation of offenses.
- Reviewed the Organizational Security Policies to implement the controls and proper Alerting.
- Provided
 - Initial Rule tuning
 - Performance monitoring
 - System health monitoring
- Provided Knowledge transfer by teaching the foundations and administration Course of Qradar.
- Provided 24 x 7 SOC services to lead to advanced tuning, security event monitoring, and detection

Lasership

- Performed the Complete Requirement Gathering for the Client.
- Provided the definition, planning, and implementation of QRadar.
- Provided the documentation of AS-IS and TO-Be phases as well as the success criteria for the project completion.
- Identified the Assets of the organization for the gathering of logs and Flows.
- Performed Data Classification for the Client to access the auditing requirements.
- Created a process of Mapping said assets to Asset owners for proper escalation of offenses.
- Reviewed the Organizational Security Policies to implement the controls and proper Alerting.
- Provided
 - Initial Rule tuning
 - Performance monitoring
 - System health monitoring
- Provided Knowledge transfer by teaching the foundations and administration Course of Qradar.
- Provided 24 x 7 SOC services to lead to advanced tuning, security event monitoring, and detection

MyEyeDr

- Performed the Complete Requirement Gathering for the Client.
- Provided the definition, planning, and implementation of QRadar.
- Provided the documentation of AS-IS and TO-Be phases as well as the success criteria for the project completion.
- Identified the Assets of the organization for the gathering of logs and Flows.
- Performed Data Classification for the Client to access the auditing requirements.
- Worked on the PII requirements for the client and helped with HIPPA compliance.
- Created a process of Mapping said assets to Asset owners for proper escalation of offenses.

- Reviewed the Organizational Security Policies to implement the controls and proper Alerting.
- Provided
 - Initial Rule tuning
 - Performance monitoring
 - System health monitoring
- Provided Knowledge transfer by teaching the foundations and administration Course of Qradar.
- Provided 24 x 7 SOC services to lead to advanced tuning, security event monitoring, and detection

Established SOC Center for SPS

- Provided SME level technical and strategic direction to the SIEM team
- Design, build and deliver training to the SIEM team and SOC on QRadar
- Designed and Managed all highly complex workloads and SOPs followed by the SOC in line with the Customer requests.
- Design, document, and implement processes and procedures for SOC.
- Performed QRadar product support and implementation for 4 different Customers.
- Monitor and maintain overall system health of supported QRadar systems until the completion of the Contract.

IT Support Manager

- Responsible for Life Cycle Support of all Internal IT Assets that include Maintenance,
- Administration, Monitoring, and Management of Assets.
- Internal Information Technology Manager responsible for all Network Operations within SPS, which includes Installation and Configuration of Servers, Internal Project Web Sites, Desktops and Laptops, as well as Software Configuration and Control.
- Upgraded old Windows Server 2003 AD to 2016 and provisioned ADCs.
- Upgraded Sage from Windows Server 2003 to 2016
- Continuous Data Production-Implementation of CDP from unified storage management
- IT Runbooks
- Custom configuration of newly assigned machines including laptops
- Lifecycle management of user on Active Directory
- Managing multiple ISPs and providing singular network
- Managing both wired and wireless networks
- Assisted various teams with my Tivoli expertise. The major contribution was with the BMW team.

COURSES / CERTIFICATIONS

IBM Security QRadar Certifications

- IBM Certified Associate Administrator - Security QRadar SIEM V7.2.8

Other Certifications

- IBM Certified Administrator - Security Guardium V10.0
- IBM Certified Solution Advisor - Tivoli Service Delivery and Process Automation Solutions V3
- IBM Certified Solution Advisor - Tivoli Storage Solutions V3
- IBM Certified ADP - IBM Service Management Tivoli Storage Management Solutions V3
- IBM Certified Associate - Tivoli Storage Manager v6.2
- IBM Certified Deployment Professional - Tivoli Storage Manager Fastback V6.1.1
- IBM Certified Deployment Professional - Tivoli Storage Manager V6.2
- IBM Certified Deployment Professional - Tivoli Storage Productivity Center V4.2
- IBM Information Management DB2 Technical Professional v2
- IBM Certified ADP - IBM Service Management Tivoli Storage Management V4
- IBM Certified Database Administrator - DB2 9.7 for Linux, UNIX, and Windows
- IBM Certified Database Associate -- DB2 9 Fundamentals
- IBM Certified Deployment Professional - Tivoli Endpoint Manager V8.2
- IBM Certified System Administrator - WebSphere Application Server Network Deployment V7.0
- Microsoft Certified Solutions Associate
- Oracle 11g DBA

IBM Security QRadar Courses Taught

4. IBM Security QRadar SIEM 7.2 Administration and Configuration (BQ121G)
5. IBM Security QRadar SIEM Foundations (BQ102G)

Other IBM Courses Taught

6. IBM BigFix Platform Foundations (IS720G)
7. IBM BigFix Content Development (IS730G)
8. Custom IBM IBM BigFix Lifecycle, Inventory, Compliance, and Patching classes
9. IBM Tivoli Monitoring 6.3 Fundamentals (TM023G)
10. Custom IBM MaaS360 class.

Name	DIANE YINGLING
Project Role	QA AND TESTING LEAD
Years of Experience	25

DIANE YINGLING – QA AND TESTING LEAD

As a QA and Testing Lead Diane Yingling specializes in Identity and Access Management (IAM) products, she has successfully overseen the quality assurance processes for multiple IAM projects throughout her 25 years of career. Her leadership involved managing dedicated testing teams, implementing rigorous testing methodologies, and ensuring the seamless integration of IAM solutions. She played a pivotal role in developing and executing comprehensive test plans, encompassing functionality, security, and scalability testing for IAM products. Additionally, she has effectively communicated testing outcomes to cross-functional teams, ensuring alignment with project objectives and client expectations in the ever-evolving landscape of IAM solutions

PROFESSIONAL EXPERIENCE

With a seasoned background in QA and Testing, she brings a wealth of experience to the table. Her expertise lies in effectively leading a QA team and ensuring a successful project. With exceptional writing and communication skills, she has consistently demonstrated the ability to convey complex concepts effectively to clients, partners, and team members alike. Her strong organizational skills enable her to seamlessly manage multiple tasks, even under pressure, ensuring optimal project coordination and delivery. Proficient in Microsoft Office applications such as Excel, Word, PowerPoint, and Lync, she leverages advanced knowledge of these tools to enhance productivity, streamline processes, and contribute to the overall efficiency of the teams she led.

SOFTWARE PRODUCTIVITY STRATEGISTS, INC.

PROGRAM MANAGEMENT

- Implemented and managed processes and templates to create consistency of service and deliverables across all client projects. From 2006 to 2011, the hours supported grew 141%, Revenue increased by 93% and Margin increased by 58%.
- Managed the forecast, costs and expenses of the Virtual Technology Services business unit. Have implemented Cost Management techniques to strive for annual net profit goals.
- Created reports to analyze the business unit, including revenue and margin by customer and service type
- Manage a services delivery team of 30 who provide over 2000 hours per month to multiple clients.

- Communicate monthly with clients to ensure that the services are meeting the clients' needs and to address any issues.
- Expertise in Webex (Meetings, Training Center & Events), Zoom, HPE MyRoom, and Teams.
- Management Award in 2005
- Awarded 2011 Core Business Area of the Year for our growth in both revenue and margin over the previous year

PROJECT MANAGEMENT

- Manage Identity and Access Management projects to maximize customer value for a variety of clients, including those from Healthcare, Higher Education, and Automotive.
- Implement Service Delivery processes, standards, and templates to ensure consistency in how projects are implemented and the level of quality that the customers receive.
- Ensure that work is within scope of the project and approved prior to work beginning.
- Facilitate weekly status calls to discuss project progress, upcoming tasks, current issues, and open action items with the project team.
- Communicate and categorize issues that are found during implementation and ensure that action is taken.
- Escalate issues to clients and/or management, when necessary.

MANUGISTICS, INC.

PROGRAM MANAGEMENT

- Coordinated and managed the release planning and launch process for a \$60 million Development organization, which included over 30 products, and led a team that was responsible for the communication of product release plans.
- Instituted and managed the product management processes and templates including requirements and design, release planning, and enhancement requests used by all products to insure consistency and quality in all software releases.
- Facilitated the change request process for all products involved in each release, bringing together the key decision makers from Engineering, Marketing and Product Management to insure consensus on the decisions that were made.
- Awarded President's Club Award in 2002
- Awarded Team Excellence Award by Executive Management in 2002

PRODUCT MANAGEMENT

- Managed the requirements & design process, release planning, and enhancement requests for Supply Planning product, Constraint Based Master Planning.
- Worked with clients to understand their business pains and requirements while developing Use Cases for future product features and functions.
- Regularly presented product release plans and client success stories to hundreds of participants at user and partner conferences.

SENIOR TRAINER

- Established and coordinated curriculum, from needs assessment through course materials for all Supply Chain application courses.
- Developed and delivered instructor led classroom and distance learning training to over 800 new employees, partners and clients on Supply Chain products.
- Developed training to support Project Management and new implementation methodology to be used by all implementation consultants.
- Assisted in the development of a new corporate training department.
- Awarded Trainer of the Year in 1998, which was selected by learners who attended my classes.
- Awarded Team Excellence Award in 1998 by Executive Management.

SUPPLY CHAIN CONSULTANT

- Led, managed, and implemented complex solutions to address client business objectives and priorities as they related to Supply Chain Management.
- Proven ability to deliver results for the client, including a reduction in inventory and improved service levels.
- Subject matter expert in Manugistics' products, with a focus on Supply Chain Planning and Optimization.

Name	FARHAN FIDA
Project Role	MOBILE APPLICATION DEVELOPER
Years of Experience	7

FARHAN FIDA – MOBILE APPLICATION DEVELOPER

As a mobile application developer Farhan is responsible for designing, developing, and maintaining applications for mobile devices, such as smartphones and tablets. His role involves collaborating with cross-functional teams to understand project requirements, translating these into functional and user-friendly mobile applications. He utilizes programming languages such as Java, Swift, or Kotlin, along with various development frameworks, to create efficient and responsive apps. He also ensures optimal performance, usability, and security of the applications, conducting testing and debugging as needed.

PROFESSIONAL SUMMARY

In his 7 years Fida is actively involved in developing RESTful Web Services for an identity management system, working with technologies such as ISIM, Azure AD, MS AD, QRadar, and Sophas. Additionally, he has contributed to the development of Android and iOS mobile apps for the same identity management system.

MOBILE APPLICATION DEVELOPER EXPERIENCE

Software Productivity Strategists, Inc.

- Develop RESTful Web Services for an identity management system
- Worked with ISIM, Azure AD, MS AD, QRadar, Sophas
- Developed Android and IOS Mobile Apps for an identity management system

Doorstep E-commerce Int.

- Designed and Developed Mobile apps (Android & IOS) for the e-commerce platform.
- Developed Admin Dashboard.

CorgInffinitg

- Supported CoreInfinite software development & testing processes. Worked on over 30 Android native Applications
- Worked with custom APIs, realtime location and camera apps. Designed UI concepts for apps and front-end development.
- Worked on Java Based Desktop Simulatio Apps

Selected for IBM Global Entrepreneur

- Developed a personalised ads targeting advertisement engine using IBM Watson

ACHIEVEMENTS

National Development Awards

- Tactics 2015
- Visio Spark 2016
- TechSalvo 2016
- TechSalvo 2017
- TechSalvo 2018
- E-Rozgar Hackathon 2018
- Visio Spark 2018
- Air Tech 2018
- Air Tech 2019
- Innovatia 2019

Name	MUSSA KHAN SHAUKAT
Project Role	WEB APPLICATION DEVELOPER
Years of Experience	3

MUSSA KHAN SHAUKAT – WEB APPLICATION DEVELOPER

As a web application developer, Mussa Khan is tasked with the end-to-end development and maintenance of web applications. This involves analyzing requirements, designing the application architecture, and writing code using programming languages like JavaScript or Python. Mussa is responsible for thorough testing, ensuring proper deployment, and ongoing maintenance to address bugs and optimize performance. Collaboration with team members, documentation of code and architecture, and staying updated with the latest web development trends are integral aspects of his role.

PROFESSIONAL SUMMARY

Mussa Khan has held roles ranging from Jr. Software Engineer to Front End Developer and currently serves as a Web Application Developer. His experience spans from November 2020 to the present, with remote positions at various companies, showcasing proficiency in software engineering, front-end development, and web application design

WEB APPLICATION DEVELOPER EXPERIENCE

Software Productivity Strategists, Inc.

- designs, codes, and maintains web applications, ensuring their functionality, performance, and responsiveness.

AEGISPEAK

- implements the user interface and user experience of a website or web application, focusing on the visual elements and interactivity that users interact with directly.

NOVEX TECHNICAL SERVICES LLC

- assists in the development, testing, and maintenance of software systems, working under the guidance of senior engineers to contribute to the overall software development life cycle.

HALALOUTLET

- Designs and executes the user interface and user experience for a website or web application, concentrating on the visual components and interactivity that users engage with directly.

CERTIFICATIONS

- REACTJS
- SERVER ADMINISTRATION
- DOCKER
- KUBERNETES

Name	NAYAB AKBAR
Project Role	IBM DEPLOYMENT PROFESSIONAL AND INSTRUCTOR
Years of Experience	12

NAYAB AKBAR – IBM DEPLOYMENT PROFESSIONAL AND INSTRUCTOR

With over 12 years of comprehensive experience in the field of IBM Security Identity and Access Management (IAM), Nayab has excelled in multifaceted roles as a BM Security Solutions Advisor, IAM Consultant, Deployment Professional, and IBM training Instructor. His expertise spans strategic advisory for IAM solutions, hands-on deployment, and the facilitation of impactful training programs. As a Deployment Professional, He has successfully integrated IBM Security solutions into diverse IT environments, ensuring optimal performance and security. Additionally, his role as an IBM training Instructor reflects a commitment to knowledge sharing, empowering fellow professionals with the skills needed to navigate the complexities of IAM. His dedication to staying current with industry trends positions me as a dynamic professional ready to address the evolving challenges in the IAM landscape.

PROFESSIONAL SUMMARY

Over the course of his career as an IBM Identity and Access Management (IAM) Consultant, he has demonstrated proficiency in designing, implementing, and supporting IAM solutions for various clients. Additionally, he has served as an IBM Professional Training Instructor for various clients, delivering hands-on training in IBM Security and Governance solutions.

PROFESSIONAL EXPERIENCE

Fairfax County, Virginia (August 2018 - Present)

- Created an IAM framework, focusing on Privileged Identity Management.
- Set up Privileged Identity Management and Advanced Access Profiles using IBM Security products.
- Provided customer training, enablement, and Level 3 production support.

MyEyeDr. (February 2014 - Present)

- Implemented IAM framework with a focus on securing passwords for insurance websites.
- Established Privileged Identity Management and administered Advanced Access Profiles.
- Conducted training, enabled deployment across 200+ locations, and provided ongoing support.

University of Nevada, LAS VEGAS (March 2014 - Present)

- Integrated Identity Manager with customer applications.
- Provided ongoing support and collaborated with IBM Customer support to resolve high-priority issues.
- Developed IAM framework and implemented lifecycle processes.

Asplundh, Tree Cutting Experts (August 2014 - Present)

- Installed and supported IBM Security products for development and production environments.
- Integrated Identity Manager with customer applications and facilitated IAM lifecycle processes.

Loudoun County, VA (August 2013 - Present)

- Installed and supported IBM Security products, focusing on Identity Manager integration.
- Established Password Synchronization and IAM lifecycle processes.

Charmers Sunbelt Group (CS-G) - Beverages Corporation (March 2014 - December 2015)

- Developed and implemented Privileged Identity Management, including training and cross-platform deployment.

Pakistan Mobile Communications Limited – Mobilink (May-July 2014)

- Conducted training and played a key role in deployment architecture for Web Access Management.

Pak Telecom Mobile Limited, Ufone (June 2012 - December 2014)

- Developed IAM Runbooks, audited current processes, and conducted a gap analysis.

MVP HealthCare – US (August 2017)

- Delivered a three-day training class, providing hands-on labs and engaging in solution discussions to address client-specific challenges.

Flushing Bank – US (August 2017)

- Conducted a three-day training class, guiding students through hands-on labs and addressing the unique issues within the client's environment.

Classified Organization (June 2017)

- Delivered a three-day training class, facilitating hands-on labs, and engaging in solution discussions tailored to the classified organization's needs.

Manitoba Public Insurance – Canada (February 2017 and April 2017)

- Provided training over two sessions, delivering hands-on labs and addressing specific challenges within Manitoba Public Insurance.

Recology – United States (December 2016)

- Delivered a three-day training class, incorporating hands-on labs and solution discussions to meet Recology's requirements.

KPMG – United States (October 2016)

- Conducted training on administration and deployment, involving hands-on labs and solution-focused discussions tailored to KPMG's context.

Bank Hapoalim – New York, United States (December 2015)

- Delivered fundamental training, including hands-on labs, and engaged in solution discussions to address the specific needs of Bank Hapoalim.

CERTIFICATION/COURSES

- IBM Mobile Customer Engagement - [REDACTED]
- IBM Marketing Cloud - [REDACTED]
- IBM Information Management Data Security & Privacy - [REDACTED]
- IBM Security People and Cloud - [REDACTED]

Name	SAQIB KIANI
Project Role	IDENTITY MANAGEMENT DEPLOYMENT SPECIALIST
Years of Experience	16

SAQIB KIANI – IDENTITY MANAGEMENT DEPLOYMENT SPECIALIST

Saqib has been serving as an IAM (Identity and Access Management) deployment security consultant since 2004. In his capacity as an IAM Consultant, he fulfills diverse roles such as an IBM Security Solutions Advisor and Deployment Professional. His extensive experience encompasses providing strategic advice on IBM Security Solutions and actively participating in the deployment process. Saqib's role involves not only consulting on IAM strategies but also hands-on implementation as a Deployment Professional, ensuring the effective integration and optimization of security solutions.

PROFESSIONAL SUMMARY

Over the last 16 years, Saqib has dedicated himself to supporting SPS customers in the comprehensive process of planning, designing, and implementing Identity Management solutions. Proficient in a wide array of technologies and tools, including IAM solutions, QRadar, Guardium, BigFix, MaaS360, ISIPM, ISIM, Thycotic Secret Server, ITIM, and more, he brings a wealth of expertise to ensure successful solution implementation for client.

IDENTITY MANAGEMENT DEPLOYMENT EXPERIENCE

Asplundh Tree Experts - IAM - IBM ISIM, ISAM, TDI

- Led the team to upgrade ISIM, ISAM, TFIM from 2014 versions to 2018 versions
- Upgraded entire IAM environment of 60,000+ users in less than 6 months, with less than 50 support calls on the cutover day
- Helped Asplundh reduce their helpdesk costs by 70% by implementing a customized ISIM self-service application
- Helped integrate over 12 Cloud services using SAML 2.0, OpenID, and WS Federations
- Integrate 2FA with ISIM self-service application

Asplundh has been a reference customer since 2014

University of Nevada Las Vegas (UNLV) - IBM Security Identity, Access & Single Sign-On

- Architect, Design, and Implement ISIM, ISAM, TFIM & QRadar
- Implement role-based provisioning, de-provisioning, access, single sign-on, and privileged user management
- Upgrade ISIM, ISAM, TFIM to the latest versions (as of 2018)
- Develop and implement Self-Service application using ISIM REST APIs
- Integrate 2FA with ISIM self-service application
- ISIM, ISAM, IGI training for UNLV staff
- Implement IBM Cloud Identity
- Helped integrate over 15 Cloud services using SAML 2.0, OpenID, and WS Federations
- QRadar Deployment, Log Sources Integration & Training

My Eye Doctor - ISPIM, QRadar, Guardium, ISIM, MaaS360, Thycotic Secret Server

- Testing, Configuration, Implementation, LDAP, SIGNA Profiling
- Password Management for SSO - Take VM backups and Snapshots
- Gather the support files before upgrade
- Collect certificates information
- Assemble ISPIM V2.0.1 virtual Appliance upgrade package with existing ISPIM Appliance V2.0.0.0
- Transfer firmware to virtual storage of the installed appliance
- Set the second partition as an active partition
- Format the secondary partition
- Security Identity Management - Validate System Architecture
- Finalize Production Environment
- Privileged Identity Manager - Production Rollout to all users and Internal Walkthrough
- Data Protection using Guardium – Configure and deploy policies and alerts
- QRadar Deployment & Integration
- Managed Security Services including 24x7 Security Operations Center (SOC)

Charmers Sunbelt (CS)

- PIM LDAP and DB2 configs with the appliance
- SessionRecording configs with ISPIM appliance/ DB2 and LDAP config
- SessionRecording configs with ISPIM appliance/ DB2 and LDAP config
- PIM appliance set up for Dev environment - LDAP configs
- PIM pre-configured VM setup

Loudoun County Government, Leesburg, Virginia - ITIM

- Plan, design, architect & lead the team of implementers to deploy IBM ISIM, ISAM ESSO and IBM Privileged Identity Manager at Loudoun County
- Added IDI data feed on ITIM server to query IDI for an identity feed and tested to ensure communication between ITIM server and IDI
- Re-imported CSV data into ITIM

- Integrate 2FA with ISIM self-service application
- Documented specs for servers
- Created organizational roles, provisioning policies and services in ITIM for various database applications
- Provided analysis of the implementation of background execution of IDI assembly lines
- Created start/stop script to control LDAP tracing
- Installed IBM recommended solution to LDAP hang problem
- Worked on ITIM documentation
- Upgraded ITDI to 6.0 and applied FIX PACK 1 for ITDI 6.0
- Created start/stop script for IDI
- Resolved the Java plug-in issue for ITIM
- Interviewed system administrators to identify provisioning policies
- Provisioned and tested provisioning of users in ITIM and SAP
- Worked on ITIM org tree management
- Authored various scripts for Windows environment
- Lead the team to plan and execute ISIM upgrade with minimum impact to end-users
- Design, architect and implement user self-service application using ISIM REST APIs
- Currently Supporting ISIM operations & expansion

LCVA is a reference customer since 2014.

Insight Communications, Louisville, KY

- Worked on Unified single sign-on to Insight Webservices

Anakam – San Diego, CA

- Worked on the analysis, requirements, and design of the project.
- TFA - TIM Resource Adapter development

Carmax – Richmond, VA

- Worked on ITIM integration and IMS Upgrade services

Department of Human Services, Hawaii

- Worked on Customization, user self-service, centralized auditing & reporting

Telenor, Pakistan

- Reviewed and documented ACS architecture and ACS identity life cycle.
- Installed and configured ACS adapter in Development and Production Environment.
- Created ACS service, policies, and rules in the development and production environment.

- Installed and configured ACS and ACS adapter on an independent machine with multiple processors to test performance and memory leakage.
- Configured provisioning parameters for ACS.
- Documented the process and took backups for ACS.
- Created roles, provisioning policies, identity policies, and password policies for ACS in the production environment
- Worked on ACS reconciliation and adoption rules.
- Supported Telenor admins for testing on the production environment.
- Provided training on the integration of ITIM and ACS.
- Created a custom adapter for TRACKER application and integrated it with ITIM
- Created: New ITIM profile, a test Tracker service, test role, and provisioning policy, a test person and Tracker account, Adoption Policy for Tracker on ITIM (Dev) and Test
- Reconciled the Tracker Service on ITIM (Dev) and Test
- Moved Solution to Staging from the test environment
- Eliminated data redundancy on staging(100 records for testing)
- Reconciled the tracker service with staging
- Created and tested: Profile for a tracker, new object class for Franchise User type, approval workflow for Franchise user for AD, approval workflow for Tracker user, a dynamic role for Franchise user, e-mail notification templates for AD and Tracker workflow ---- (Production TIM)
- Reconciled the tracker service, AD service for Franchise domain (Production TIM)
- Created & tested ACI, Views, Groups for helpdesk (Tracker Franchise, Telenor employees)
- Executed acceptance tests Production)
- Ran reconciliation for Tracker Service & AD Franchise

SHAW, Inc

- ITIM Workflow Extension (ChangeAddLastName Operation)

Publishers Press

- Preparing the Baseline Document
- Installation & Configuration document preparation

Maines

- Preparing the Baseline document.

Legg Mason, Owings Mills, Maryland

- Preparing the Design document for ITIM Implementation
- Preparation of SPNEGO document

Teknor Apex

- Preparing the “Plan for Teknor Apex Workflow extension” Document
- Preparing TIM Architecture Diagram
- Preparing TAM Architecture Diagram

CERTIFICATIONS

IBM Certifications:

- IBM Tivoli Identity Manager 5.1 Implementation
- IBM Tivoli Identity Manager 4.6
- IBM WebSphere MQ V7.0 System Administration
- IBM Tivoli Compliance Insight Manager V8.5
- IBM Tivoli Security and Compliance Management Solutions V2
- IBM Tivoli Access Manager for Enterprise Single Sign-On V8.0.1

Oracle Certified:

- Developer Track
 - Paper –I SQL
 - Paper-II PL/SQL
- DBA Track
 - Paper –I SQL
 - Paper-II Fundamental I
 - Paper – III Fundamental II

Name	SHAHAB AKBAR
Project Role	IAM DEPLOYMENT PROFESSIONAL
Years of Experience	03

SHAHAB AKBAR – IAM DEPLOYMENT PROFESSIONAL

As an IBM IAM professional Shahab plays a pivotal role in safeguarding organizational security and efficiency by managing user identities and controlling access to IT resources. Responsibilities encompass user provisioning, authentication methods implementation, access control enforcement, and integration with existing systems. He is tasked with ensuring adherence to security policies, compliance regulations, and risk management practices. As an IAM professional Shahab also contribute to the deployment and maintenance of IAM systems, staying informed about the latest trends, and continuously optimizing processes to enhance overall security posture. Their multifaceted role requires technical expertise, a deep understanding of security principles, and effective communication to align IAM solutions with organizational goals.

PROFESSIONAL EXPERIENCE

Over the past 3 years as an IBM IAM Implementor and Deployment Professional, he has gained extensive experience in supporting, administering, and integrating IBM Security Identity and Access Management solutions. He has successfully implemented IBM PAM and IAM solutions for both local and offshore clients, facilitating integrations with databases, directory servers, and applications. Additionally, his role involved participation in the implementation of IBM Secret Server for various customers. He actively collaborated with HR to identify business development opportunities and demonstrated project coordination skills.

IAM DEPLOYMENT PROFESSIONAL EXPERIENCE

Cyber Security Analyst - Software Productivity Strategists, Inc.

- IBM IAM Implementor as Deployment Professional
- IBM PAM Implementor as Deployment Professional
- IBM based Identity and Access Management Support and Administration.
- IBM Security Identity and Access Management solution integrations with targets such as Databases, Directory Servers, Applications.
- Participated in implementation for the IBM Secret Server for local and offshore customers.
- Worked with HR to create opportunities for business development.
- Project Coordination and customer satisfaction management.
- Project profitability management and reporting.

In SPS Shahab us working as an IAM consultant for various local + international customers. His responsibilities are Administration, Support and Reporting.

Utilities based company in Pennsylvania, US

- Identity Management and Access Management and Privilege Access Management

University in Las Vegas, US

- Identity Management and Access Management.

Local bank in Pakistan

- Identity Management, Access Management and Privilege Access Management.

Eyecare company in California

- Privileged Access Management, deployment, and support

Utilities based company in Maryland, US

- Privileged Access Management, deployment, and support

COURSES/ CERTIFICATIONS

- IBM Security Sales Foundations issued by IBM
- IBM Cloud Pak for Security Sales Foundations issued by IBM
- Sales Foundations for IBM SaaS issued by IBM
- Cybersecurity Fundamentals issued by IBM
- Working in a Digital World: Professional Skills issued by IBM
- Data Science for Business - Level 1 issued by IBM
- Enterprise Design Thinking Practitioner issued by IBM
- IBM Cloud Pak for Security v1.x Administrator Specialty

Name	TAISH HASSAN KHAN
Project Role	SIEM DEPLOYMENT PROFESSIONAL
Years of Experience	03

TAISH HASSAN KHAN - SIEM DEPLOYMENT PROFESSIONAL

Taish is a seasoned expert in SIEM deployment, currently engaged with various clients and utilizing multiple tools such as QRadar, Guardium, and BigFix. Proficient in identifying vulnerabilities and weaknesses within client network infrastructures, Taish excels in log analysis, demonstrating strong critical thinking and effective communication skills. Additionally, adept at reviewing customer queries, Taish provides guidance on threat remediation strategies and advocates for best security practices.

PROFESSIONAL EXPERIENCE

In the last three years at SPS, Inc., he has shouldered cybersecurity responsibilities for multiple clients, showcasing expertise in diverse areas, notably with the SIEM Tool IBM QRadar. His role encompasses deployment, patch management, vigilant alert monitoring, and effective use case implementation. Excelling in SOC operations, he adeptly performs log analyses, flow analyses, correlation, and anomaly detection, contributing to the generation of audit reports. Proactively fine-tuning correlation rules, he minimizes false-positives and responds promptly to incidents. Specializing in client-specific historical incident analysis, he aids in identifying and remediating security vulnerabilities. Furthermore, he manages QRadar maintenance, troubleshooting, patching, and the seamless integration of new extensions

SIEM Deployment Experience

MyEyeDr – QRadar

- Worked in 24/7 rotational shifts to carry out SOC Monitoring services
- Logs and Flows analyses of different devices like Windows, Servers, Applications, Routers, Firewalls, etc. In-depth investigation and escalation of offenses
- Health Monitoring (FPS, EPS limits, GUI, CLI availability, Validation of Disk space)
- Deployment, upgrades, and patches of QRadar
- QRadar Rules tuning and modifications of Building blocks to mitigate false positives
- Integration of Log sources with IBM QRadar with different protocols especially WinCollect (used for the collection of Windows Events)
- Installation and configuration of different app extensions with QRadar like UBA, QDI, Vulnerability Insight, Threat Intelligence, and Content Extension for Sysmon, etc
- Addition of Network Hierarchy, Users and Licenses Management, Backup and Recovery Management (Config and Data backups), Reference Set Management, Asset Management, Configuration and Scheduling of Reports
- Installation and Configuration of WinCollect Agent and its up-gradation to latest patches
- Custom Regex to extract any specific data field from Payloads

- Managing customized events/flows searches and clearing searches using CLI if stores got filled more than threshold limits

Lasership – QRadar

- Worked in 24/7 rotational shifts to carry out SOC Monitoring services
- QRadar administration tasks
- Weekly Offenses meeting with the client and taking care of meeting minutes and follow up of action items

Asplundh Tree Expert, LLC – QRadar

- Worked in 24/7 rotational shifts to carry out SOC Monitoring services
- Generating Tickets using ServiceNow for the critical incidents
- QRadar administration tasks
- Weekly Offenses meeting with the client and taking care of meeting minutes and follow up of action items

Altria Group, Inc – QRadar

- Working in 24/7 rotational shifts to carry out SOC Monitoring services

COURSES / CERTIFICATIONS

- IBM QRadar Associate Analyst v 7.2.7 – Training
- IBM QRadar Associate Administrator v 7.3- Training

Name	ZAHRA KHAN
Project Role	QUALITY ASSURANCE ENGINEER
Years of Experience	12

ZAHRA KHAN – QUALITY ASSURANCE ENGINEER

With a comprehensive 12-year background in manual testing, Zahra has garnered substantial expertise in evaluating various software platforms, including mobile, web, and desktop applications. Her proficiency extends across a diverse array of testing types, including exploratory, smoke, sanity, regression, adhoc, and stress testing. This wealth of experience positions her as a seasoned professional capable of ensuring the quality and reliability of software systems across different domains.

PROFESSIONAL SUMMARY

A highly skilled and detail-oriented Software Quality Assurance (SQA) Engineer with over 12 years of hands-on experience in manual testing. Proven expertise in evaluating the quality and functionality of diverse software applications, including mobile, web, and desktop platforms. Proficient in various testing types, such as exploratory, smoke, sanity, regression, adhoc, and stress testing. Adept at collaborating with cross-functional teams to identify and rectify defects, ensuring the delivery of high-quality software products. Possesses a strong commitment to quality assurance standards and a track record of consistently improving testing processes. A seasoned professional dedicated to ensuring the reliability and performance of software systems throughout the development lifecycle.

QUALITY ASSURANCE EXPERIENCE

Software Quality Assurance Lead:

- Assignment distribution
- Team coordination
- Test team's primary contact
- Allocating resources
- Resolving issues
- Conducting interviews for new hires
- Onboarding new hires through training
- Development of training materials
- Engaging with senior management

- Daily review of testers' work
- Compiling test results
- Communicating results to relevant stakeholders.

Software Quality Assurance Engineer

- Executing Sanity, Regression, and Ad hoc testing across various platforms
- Recognizing and documenting observed issues as bug reports
- Offering comprehensive guidance including annotated screenshots, logs, and pertinent data for bug reports
- Create and publish comprehensive daily progress reports, which include outcomes of individual test cases.
- Validating bugs across different platforms for consistency
- Verifying resolved bugs after fixes are implemented.
- Compiling test cases for newly introduced features or revising existing ones to incorporate feature modifications.
- Adhere to client and project manager's designated timelines and testing rate objectives.
- Promptly address requests for additional information or verification testing.

CRFP ERP24-02 Designated Contact

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) Mary Stang / Director - Local, State, Education

(Address) 2400 Research Blvd. Suite 115, Rockville, MD 20850

(Phone Number) / (Fax Number) 301-337-2290 / NA

(email address) mary.stang@spsnet.com

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

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

Software Productivity Strategists, Inc. _____

(Company) 

(Signature of Authorized Representative)
Director - State, Local, Education

(Printed Name and Title of Authorized Representative) (Date)
301-337-2290 / NA

(Phone Number) (Fax Number)
mary.stang@spsnet.com

(Email Address)

CRFP ERP24-02 Availability of Information

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

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 – $1 \times 30 =$ 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 – $0.909091 \times 30 =$ 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.


Software Productivity Strategists, Inc.
(Company)

Mary Stang, Director – State, Local Education
(Representative Name, Title)

301-337-2290
(Contact Phone/Fax Number)

March 16, 2024
(Date)

CRFP 0947 ERP240000002 2 WV CRFP FORM

	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: To post addendum 01.		
Doc Description: Identity Management Single Sign-On Solution			
Proc Type: Central Master Agreement			
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: VS0000019723

Vendor Name : Software Productivity Strategists, Inc.

Address :

Street : 2400 Research Blvd. Suite 115

City : Rockville

State : Maryland

Country : USA

Zip : 20850

Principal Contact : Mary Stang

Vendor Contact Phone: 301-337-2290

Extension: NA

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

Vendor Signature X 

FEIN# 52-1832154

DATE 03/13/2024

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

	Document Phase	Document Description	Page
ERP240000002	Final	Identity Management Single Sign-On Solution	3

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

CRFP ERP24-02 - Addendum 01

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

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: VS0000019723
Vendor Name : Software Productivity Strategists, Inc.
Address :
Street : 2400 Research Blvd. Suite 115
City : Rockville
State : Maryland **Country :** USA **Zip :** 20850
Principal Contact : Mary Stang
Vendor Contact Phone: 301-337-2290 **Extension:**

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

Vendor Signature X  **FEIN#** 52-1832154 **DATE** 03/20/2024

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.

Revised 6/8/2012

ATTACHMENT A

Revised 6/8/2012

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:

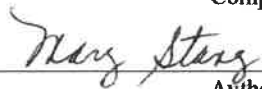
(Check the box next to each addendum received)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> 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.

Software Productivity Strategists, Inc. _____

Company

 _____

Authorized Signature

03/20/2024 _____

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.
Revised 6/8/2012

CRFP ERP24-02 - Addendum 02

	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		Reason for Modification: 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 ERP240000002	3

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code: VS0000019723
Vendor Name : Software Productivity Strategists, Inc.
Address :
Street : 2400 Research Blvd. Suite 115
City : Rockville
State : Maryland **Country :** United States **Zip :** 20850
Principal Contact : Mary Stang
Vendor Contact Phone: 301-337-2290 **Extension:** N/A

FOR INFORMATION CONTACT THE BUYER

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

Vendor Signature X *Mary Stang* **FEIN#** 52-1832154 **DATE** 03/29/2024

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.

Revised 6/8/2012

ATTACHMENT A

Revised 6/8/2012

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

Version 11-1--19

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.

Version 11-1--19

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,

Version 11-1--19

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

Version 11-1--19

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.

Version 11-1--19

- 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

Version 11-1-19

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

Version 11-1--19

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

Version 11-1--19

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

Version 11-1--19

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.

Version 11-1--19

AGREED:

Name of Agency: _____

Name of Vendor: Software Productivity Strategists, Inc.

Signature: _____

Signature: Mary Stenz

Title: _____

Title: Director - State, Local, Education

Date: _____

Date: 03/29/2024

Version 11-1--19

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)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> 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.

Software Productivity Strategists, Inc.

Company



Authorized Signature

03/29/2024

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012