

TECHNICAL PROPOSAL PACKET
SP-21-0029

REDACTED

PROPOSAL SIGNATURE PAGE

Type or print the following information

PROSPECTIVE CONTRACTOR'S INFORMATION					
Company:	TechDemocracy LLC				
Address:	1 Corporate Place South, Suite # 110				
City:	Piscataway	State:	NJ	Zip Code:	08854
Business Designation:	<input checked="" type="checkbox"/> Individual <input type="checkbox"/> Sole Proprietorship <input type="checkbox"/> Public Service Corp <input type="checkbox"/> Partnership <input type="checkbox"/> Corporation <input type="checkbox"/> Nonprofit				
Minority and Women-Owned Designation*:	<input type="checkbox"/> Not Applicable <input type="checkbox"/> American Indian <input type="checkbox"/> Service Disabled Veteran <input type="checkbox"/> African American <input type="checkbox"/> Hispanic American <input checked="" type="checkbox"/> Women-Owned <input type="checkbox"/> Asian American <input type="checkbox"/> Pacific Islander American				
	AR Certification #: _____ * See <i>Minority and Women-Owned Business Policy</i>				

PROSPECTIVE CONTRACTOR CONTACT INFORMATION			
<i>Provide contact information to be used for RFP solicitation related matters and Project Lead for Interview.</i>			
Contact Person:		Title:	CFO
Phone:		Alternate Phone:	
Email:			

CONFIRMATION OF REDACTED COPY
<input checked="" type="checkbox"/> YES, a redacted copy of submission documents is enclosed. <input type="checkbox"/> NO, a redacted copy of submission documents is <u>not</u> enclosed. I understand a full copy of non-redacted submission documents will be released if requested.
<i>Note: If a redacted copy of the submission documents is not provided with Prospective Contractor's response packet, and neither box is checked, a copy of the non-redacted documents, with the exception of financial data (other than pricing), will be released in response to any request made under the Arkansas Freedom of Information Act (FOIA). See RFP Solicitation for additional information.</i>

ILLEGAL IMMIGRANT CONFIRMATION
By signing and submitting a response to this <i>RFP Solicitation</i> , Prospective Contractor agrees and certifies that they do not employ or contract with illegal immigrants and shall not employ or contract with illegal immigrants during the term of a contract awarded as a result of this RFP.

ISRAEL BOYCOTT RESTRICTION CONFIRMATION
By checking the box below, Prospective Contractor agrees and certifies that they do not boycott Israel and shall not boycott Israel during the term of a contract awarded as a result of this RFP.
<input checked="" type="checkbox"/> Prospective Contractor does not and shall not boycott Israel.

An official authorized to bind the Prospective Contractor to a resultant contract shall sign below.

The signature below signifies agreement that any exception that conflicts with a Requirement of this *RFP Solicitation* may cause the **Prospective Contractor's** proposal to be rejected.

Authorized Signature: _____ **Title:** _____

Printed/Typed Name: _____ **Date:** _____

SUBMISSION REQUIREMENTS CHECKLIST

Per the RFP, the following items **must** be submitted with the Prospective Contractor's proposal:

- Proposal Signature Page*
- Proposed Subcontractors Form*
- Information for Evaluation*
 - Experience (2 pages or less)*
 - Solution (2 pages or less)*
 - Risk (2 pages or less)*
 - Value Added (2 pages or less)*
- Exceptions Form, if applicable*
- Official Solicitation Price Sheet*

It is strongly recommended that the following items are also included with the Prospective Contractor's proposal:

- EO 98-04: Contract and Grant Disclosure Form*
- Copy of Prospective Contractor's Equal Opportunity Policy*
- Voluntary Product Accessibility Template (VPAT), if applicable*
- Signed addenda, if applicable*

PROPOSED SUBCONTRACTORS FORM

- **Do not** include additional information relating to subcontractors on this form or as an attachment to this form.
 - Prospective Contractor **shall** complete and submit the *Proposed Subcontractors Form* included in the *Technical Proposal Packet*.
 - Additional subcontractor information may be required or requested in following sections of this *RFP Solicitation* or in the *Information for Evaluation* section provided in the *Technical Proposal Packet*. **Do not** attach any additional information to the *Proposed Subcontractors Form*.
 - The utilization of any proposed subcontractor is subject to approval by the State agency.

PROSPECTIVE CONTRACTOR PROPOSES TO USE THE FOLLOWING SUBCONTRACTOR(S) TO PROVIDE SERVICES.

Type or print the following information

SUBCONTRACTOR'S COMPANY NAME	STREET ADDRESS	CITY, STATE, ZIP

PROSPECTIVE CONTRACTOR DOES NOT PROPOSE TO USE SUBCONTRACTORS TO PERFORM SERVICES.

INFORMATION FOR EVALUATION – EXPERIENCE

Level of Experience:	Our IAM team is well experienced with the customer required business use cases, design, architecture, installation, configuration, support and management of IT security projects for Public Sector, Higher Education, Utility, State & Local, Federal, and commercial domain, our team understands that the client aggressively uses the internet for their employees, contractors, vendor’s services, administrative systems, self-service and profile management, thus online security plays a very significant role. We have extensive experience in Identity management, integration with upstream and downstream identity repositories, coarse and fine grain access security management based on IGA product suite.
Documented Performance:	Our IAM experts have deployed exceeding 100+ successful implementations in last several years.

Level of Experience:	With over two decades of experience developed IAM practice based on proven processes, methodologies and technology with the focus on business knowledge, experience, and specialized skill sets to ensure the success of the security projects which position us as a Unique Technology IT Risk Management Vendor in the Industry.
Documented Performance:	Implemented more than 100+ successful IAM projects and provided maintenance services to multiple clients

Level of Experience:	Rich experience in implementing IAM products with Student Information Systems such as Banner and CAS leveraging standard connector architectures.
Documented Performance:	Successful management of entitlements across the schools and universities where the IAM program was implemented.

Level of Experience:	A US City wanted to provide City employees with self service Capability and Automate On-Boarding and Off-Boarding process for Staffs and Temporary workers. It wanted to allow all city agencies to exchange information securely. We have implemented an IAM solution integrating between PeopleSoft HR, Google Apps, AD, LDAP servers and their Portal.
Documented Performance:	The implementation resulted in a Centralized Identity Store for all city agencies with self-service capabilities, lowered the cost and improved user adoption. It also improved security and efficiency by migrating manual self-service tasks to an automated system.

Level of Experience:	A US State was using a web-based ERP system which was using manual procedures for managing the users and assigning security for the applications and users were requiring different passwords to access the applications that causing additional burden on Help Desk administrators as well as users to remember. We implemented an IAM solution to automate the entire provisioning, transfers and de-provisioning process to ensure seams integration of Starters, Leavers and Movers process entered in PeopleSoft HR flowing to IAM and in turn IAM invokes the automated actions on target applications.
Documented Performance:	The State was able to significantly reduce the onboarding time for new users, while ensuring access is revoked on-time for leavers. This solution also provided users with an opportunity to use single password to manage all applications, provides self-service features e.g. Forgot Password, Change Password, Update contact information etc. which reduces help desk costs to State and improve user experience and security.

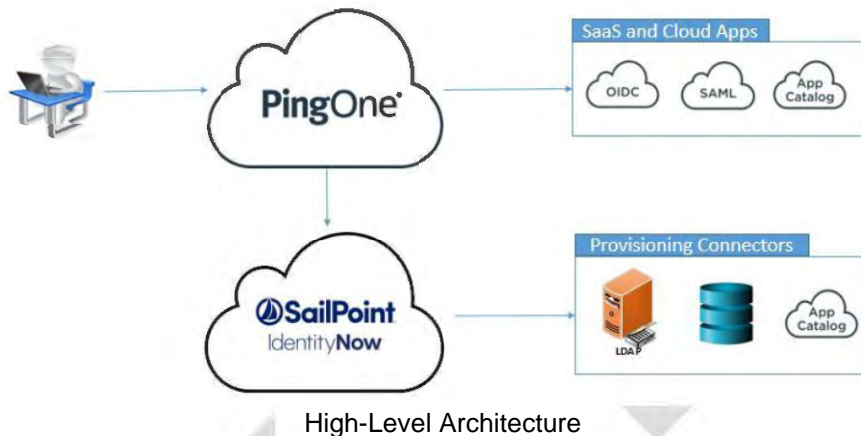
INFORMATION FOR EVALUATION – SOLUTION

Based on the requirements specified in this RFP, we propose a combination of SailPoint IdentityNow and PingOne to support the Identity Governance and Single Sign-On capabilities.

SailPoint IdentityNow

SailPoint IdentityNow is built from the ground up as a complete multi-tenant SaaS platform. Since it does not require hardware or software installation, you can rapidly and efficiently deploy and administer identity services from the cloud.

Designed with IT and security teams in mind, built-in identity best practices allow for simplified administration without the need for specialized identity expertise. All new and updated features and maintenance updates are automatically delivered to you, requiring zero downtime and IT effort. This frees up your IT resources and allows you to focus on delivering program results



IdentityNow Modules

Provisioning: Enable business users to be productive from day one. Streamline onboarding and off-boarding process with best practice configurations and workflows, enabling IT to automatically manage user access to the applications they need to perform their job.

Access Request: Empower the entire business with a self-service platform for requesting and approving access to applications, collection of entitlements within applications or application bundles, called "roles." IdentityNow secures and automates the access request process and frees IT to work on strategic projects while quickly delivering business users the access they need to do their jobs.

Password Management: Offer business users an intuitive, self-service experience for managing and resetting their own passwords from any location and on any device, on- or off-network. Leveraging industry best practices, such as sequential multi-factor authentication, this service enforces consistent and secure password policies across all systems and users in the business, while eliminating helpdesk calls and strengthening your security posture.

Access Certification: Automate the process of reviewing and reporting user access privileges across the organization. Quickly plan, schedule and execute comprehensive campaigns to ensure all types of users have the appropriate access to corporate resources.

Separation-of-Duties: Quickly create a library of policies to expose conflicts of interest and help eliminate fraud by requiring more than one individual be involved in any high-risk or sensitive task. Enforce critical risk and compliance controls by spanning policies across multiple systems and applications.

Artificial Intelligence and Machine Learning: Apply advanced governance capabilities, using the power of SailPoint Predictive Identity to discover suspicious or anomalous access, maintain continuous compliance and enjoy greater productivity across the entire organization. Utilize generated insights and recommendations to help guide decisions around your security and compliance related efforts.

Access Insights: Leverage the power of AI and machine learning to gather and analyze access information and provide rich intelligence to transform your identity program into an even greater strategic resource.

Ping One

PingOne® for Enterprise is a fast, simple and easy identity-as-a-service (IDaaS) **single sign-on (SSO)** offering that enables enterprises to give their users federated access to applications with a single click from a secure, cloud-based dock, accessible from any browser or mobile device. PingOne for Enterprise reduces user password sprawl and improves user experience, all while improving business agility and driving administrative efficiency.

PingOne for Enterprise is architected to scale, there are no practical limits to scaling the Ping Identity Platform. The Ping Solution is the most flexible on the market and are designed to scale to large number of users. Some of enterprise customers have connected 2,000+ applications to their PingOne for Enterprise accounts. With high availability and

performance. PingOne for Enterprise reliably delivers secure IDaaS solutions for the enterprise. **The Ping Solution is in production in some of the most challenging employee, consumer and partner scenarios. One CIAM client stores over 500 million user IDs in the data store. Another client uses the data store for text messaging storage with over 3 billion authentications per day.**

Identity as a Service: Provide users with single sign-on to SaaS apps leveraging a cloud-based solution that eliminates the need to set up and manage IT infrastructure. PingOne for Enterprise can be combined with PingID to rapidly add multi-factor authentication with centralized administration for both cloud-based products.

Fast and Easy Cloud App Connections: Administrators can quickly add custom applications via SAML or OIDC or use pre-configured connectors from the PingOne application catalog. If other single sign-on solutions are in use, those apps can be added to the user’s application dock for a seamless end-user experience.

Simple Administration and User Registration: Admins can connect to existing Active Directory and enable secure SSO to SaaS and cloud apps in minutes to reduce password sprawl and improve user experience. First time end users experience a seamless registration for PingOne for Enterprise. End users only need to remember one username and password and gain a centralized dock for access to all of their SaaS applications, improving security and greatly reducing help desk tickets for password resets.

Bridges Across Hybrid IT: Enterprises today are spread across on-premises and cloud infrastructure, and not every application is SaaS based. For those enterprises with a mix of applications on-premises and in the cloud, PingOne for Enterprise makes it easy to manage your journey to the cloud using variety of identity bridges designed.

Feature	Benefit
Standards Support	Supports federated identity protocols to enable SSO to SaaS applications. Standards supported: <ul style="list-style-type: none"> •OIDC, SAML 2.0 and 1.1 for authentication. •SCIM 1.1 for automated inbound and outbound user provisioning
Federated Single Sign-on	Offers standards-based, secure single sign-on. Supports dynamic user registration, centralized access control and just-in-time user provisioning. Integrates with existing identity investments and eliminates the need for multiple passwords.
PingFederate® Identity Bridge	Bridges to PingFederate® to extend IDaaS for hybrid IT use cases.
Microsoft® Active Directory Integration	Integrates with Active Directory via a small footprint agent that extends Active Directory identities to PingOne.
Identity Provider (IdP) Support	Supports user identities from PingOne Directory, Active Directory, Google Apps, PingFederate and OpenID Connect providers.
Multi-factor Authentication (MFA)	Integrates with PingID natively.
User Provisioning	Enables you to add, delete or update users at once for all applications.
Provisioning Connectors	Offers out-of-the-box integrations to connect to various applications and improve time to value.
Guided Deployment	Quick to deploy in two easy steps for 5-minute setup: <ul style="list-style-type: none"> •Select apps for your users from the thousands offered in our app catalog. •Invite users to access their apps.
End-user Portal	Delivers one-click access to applications using the included, customizable portal or an existing portal.
Mobile Applications	Provides single-click access on any device. Mobile apps available for iOS and Android.
Web-based Admin Console	Centralizes administration of application configuration, user management and reporting.
Audit Reporting	Aids analysis of security alerts by streaming audit logs to Splunk or other 3rd-party SIEM solutions.
High Availability / Disaster Recovery	Globally distributed, load-balanced and secure, with SAS70 Type II compliant data centers. Network Operations Center monitors physical and digital performance and security 24/7/365.
Security Policies	Protects transactions and data stored in PingOne with a strict set of security policies.

INFORMATION FOR EVALUATION – RISK

Risk Description:	Non-availability / Schedule Constraint of Key Stakeholders from University of Arkansas
Solution:	By listing all the dependencies, identifies stakeholders involved, and plan meetings in advance with required agenda

	University of Arkansas Project Manager to assist in ensuring the required time can be made available from the intended stakeholder
Documented Performance:	<i>The risk was mitigated at multiple customers by having a single point of contact from the customer end to reduce the schedule constraints due to non-availability of key stakeholders</i>

Risk Description:	Non-availability of environments, support from University of Arkansas and user access
Solution:	In case of unavoidable delays in provisioning support, we will make all efforts to work on other independent components of the program Any required Hardware or Software must be procured and made available to the implementation team well before the actual implementation starts, in-order to avoid any kind of delay in the delivery time-line.
Documented Performance:	<i>For one of our clients we identified the components and tasks which are not dependent on the environments availability and worked on those components to avoid losing the time and maintained the schedule as well.</i>

Risk Description:	Business stakeholders from different business units may not fully buy into migration solution due to gap in organizational change management
Solution:	Key players identified to be made available to participate in the subsequent activities per the agreed schedule University of Arkansas to ensure that logistics are in place (space, system access, security etc.) for Planning Pre-planning exercise to consolidate the information provided and to assess and improve the transition readiness
Documented Performance:	<i>The risk mitigation helped us to coordinate with key stakeholders and reduction in schedule delays due to non-availability of resources and improve transition readiness in projects</i>

Risk Description:	Uncontrolled scope increase; It can severely affect the project plan and objectives
Solution:	Proposed changes to scope will go through scope control and needs approval of both implementor/vendor and University of Arkansas Project management team before inclusion. Introducing proper change management controls and procedure or toll gates will reduce the scope creep. Also, documenting the impact of changing requirements in terms of function points, time delays or cost implications help reduce the risk.
Documented Performance:	<i>Having process toll gates helped us reduce scope creep and rework which helped us contain the schedule delay not to exceed more than 10% of the overall schedule</i>

Risk Description:	Low quality and Error prone applications or modules. User applications with number of detects poses a serious risk for the project and makes it difficult for development team to fix the bugs along with number of bugs found leading to low level of user satisfaction.
Solution:	Following "Software Quality Assurance" and "Software Quality Control" (Software testing) process we can minimize this risk significantly
Documented Performance:	<i>This is a common risk across the projects that was mitigated consistently by reducing the defect ratio and minimizing the risk of rework and schedule delays</i>

Risk Description:	Slippage in services / deliveries leading to increased cost
Solution:	We can along with University of Arkansas jointly assess the status of the project against the deliverables schedule on a weekly and monthly scale. Any deviations and inclusions outside the stated deliverables schedule will follow an escalation process

**Documented
Performance:**

This risk mitigation has been used in most of our projects where we have project assessments at regular intervals to identify issues and delays and escalate to the respective stakeholders for faster resolutions

REDACTED

INFORMATION FOR EVALUATION – VALUE-ADD

Item Claim:	Next Gen UI for Identity Manager		
How will this add value?	<p>We have built our own IDM UI solution, this solution will come with intuitive look and feel to support and integrate with any Identity Management (IDM) solution.</p> <p>Value proposition:</p> <ul style="list-style-type: none"> • Cross-Solution Integration: Integrates across multiple IDM solutions • Customizable UI: Easy to customize to align with your business needs • Proactive Analytics: Provides a strong set of data for tracking and monitoring system usage • Interoperability: Built-in integrations with rich API's • Reduced Operational Cost: Low maintenance UI 		
Documented Performance:	<p><i>The Solution was implemented based on our past experience and challenges seen in implementing the customer needs. Solution has offered and provided based on the needs of our clients and helped in achieving the requirements like</i></p> <ul style="list-style-type: none"> • <i>Multi-device support</i> • <i>Multiple IDM solution integration</i> • <i>Intuitive look and feel</i> • <i>Customizable UI with tailored dashboard</i> • <i>Simplified Request Process</i> • <i>Streamlined Access Review</i> • <i>Migration requirements, Search capability and more</i> 		
Cost Impact (%):	Minimal	Schedule Impact (%):	NA

Item Claim:	Application Onboarding Factory model		
How will this add value?	<p>We have developed an Application onboarding Factory model to facilitate rapid application onboarding. The Application Factory Model uses a standard SDLC process with well defined "cycle times" and focuses on building a repeatable and reusable model for application on-boarding.</p> <p>Key principles of the Application Factory Model include:</p> <ul style="list-style-type: none"> • Segregation of the Application into the various categories as part of the profiling and prioritization (applications of the same category will be part of a single 'wave' of on-boarding) • Entitlement warehouse to fast track the requirements gathering and definition cycle (this has been elaborated further below) 		
Documented Performance:	<p><i>The factory model has benefited our clients with:</i></p> <ul style="list-style-type: none"> • <i>Complete visibility of the list of Applications for on-boarding</i> • <i>Detailed Planning and phased roadmap for the Factory model on-boarding</i> • <i>Grouping of applications helps to fast track the on-boarding process</i> • <i>On-boarding waves can be phased in such a manner to address the business needs</i> <p><i>Outcome</i></p> <ul style="list-style-type: none"> • <i>Profiled Applications Inventory List for On-boarding</i> • <i>% reduction in Business engagement activities for each application</i> • <i>Commitment to increase number of apps on-boarded</i> • <i>Faster ROI for Business</i> 		
Cost Impact (%):	NA	Schedule Impact (%):	15% of effort reduction

Item Claim:	Center of Excellence		
--------------------	-----------------------------	--	--

How will this add value?	<p>We have built our own Center of Excellence (CoE) for Identity & Access Management. The CoE distills the rich experience that we have in IAM project implementations across different industries and ensures that we stay on the cutting edge of technology. We have developed highly complex Proof of Concepts for our clients seeking our help in Identity Management Sphere with ease. Our Research lab is building integrations between various IDM products.</p> <p>This helped us to build a connector factory which contains connectors for various products to reduce the time to deliver and build reusable components</p>		
Documented Performance:	<p><i>The COE has offered and provided Customized Identity Management solutions based on the needs of our clients and helped reduction in overall efforts which resulted lowered cost and timeline to the customers.</i></p>		
Cost Impact (%):	NA	Schedule Impact (%):	NA

Item Claim:	Intellicta		
How will this add value?	<p>Intellicta is an integrated Technology Risk Management platform that helps the board and C-Suite executives be informed about the risk posture of their organization in real-time. It helps enterprises of every size to identify and respond to the risks from enterprise systems, in both on-premises or cloud.</p> <p>Intellicta helps organizations:</p> <ul style="list-style-type: none"> • Visualize and measure the complete risk and compliance posture of their enterprise • Evaluate your security performance collectively based on the current state and against business objectives • Provides a security framework that can continuously monitor your organizational security posture • Quantify the monetary effects of potential breaches • Measure organization resiliency towards threats and vulnerabilities • Helps understand where organization stands with regards to compliance and governance standards • Enables organizations to identify the indicators of potential breaches 		
Documented Performance:	<p>TechDemocracy's Intellicta has been recognized as a Niche Player in 2020 for IT Risk Management Magic Quadrant by Gartner. Intellicta helps to enumerate the monetary effects of the potential breaches and pinpoints gaps and inefficiencies to prioritize risk investments and track progress continuously on a real-time basis.</p>		
Cost Impact (%):	NA	Schedule Impact (%):	NA

EXCEPTIONS FORM

Prospective Contractor **shall** document all exceptions related to requirements in the RFP and terms in the *Services Contract* and *Solicitation Terms and Conditions* located on the OSP website. (See Section 1.9 and 1.10 of the RFP.)

ITEM #	REFERENCE (SECTION, PAGE, PARAGRAPH)	DESCRIPTION	PROPOSED LANGUAGE
1.		None	
2.		None	
3.		None	

REDACTED

Official Solicitation Price Sheet
RFP# SP-21-0029
Identity Access Management Solution

Fields highlighted in yellow **shall** be used in calculating low price determination. Prospective Contractors **shall not** alter the Official Bid Price Sheet.

Table 1

Implementation		Total
One Time Cost	\$	298,000.00

*Provide the total, one time cost (including travel expenses) for all implementation activities necessary to fully implement the solution. The cost proposed will be an all-inclusive cost in order for the Contractor to successfully complete all implementation activities in order for the system to Go-Live.

Table 2

Annual	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Total
Licensing	\$ 628,204	\$ 628,204	\$ 628,204	\$ 628,204	\$ 628,204	\$ 628,204	\$ 628,204	\$ 4,397,430.09
Maintenance	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
Hosting	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
User & Technical Support	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -

*Provide the annual cost for licensing, maintenance, and user & technical support.

Total	\$ 4,397,430.09
--------------	-----------------

Table 3

Training		Total
One Time Cost	\$	14,000.00

*Provide the total, one time cost for completing all training activities.

Table 4

Data Conversion		Total
One Time Cost	\$	30,000.00

*Provide the total, one time cost for completing all data conversion activities.

Table 5

Customization and Enhancements (Not Evaluated)	
Hourly rate	\$ 110.00

*Provide an hourly rate for any customization or enhancements not covered by the scope of the RFP.

Table 6

Grand Total
\$ 4,739,430.09