

BID RESPONSE PACKET
710-20-0026

BID SIGNATURE PAGE

Type or Print the following information.

PROSPECTIVE CONTRACTOR'S INFORMATION					
Company:	Automation Designs & Solutions, Inc. d/b/a AD&S, Inc.				
Address:	1070 Lake Village Circle, Suite D				
City:	Brandon	State:	MS	Zip Code:	39047
Business Designation:	<input type="checkbox"/> Individual <input type="checkbox"/> Sole Proprietorship <input type="checkbox"/> Public Service Corp <input type="checkbox"/> Partnership <input checked="" 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"/> Asian American <input type="checkbox"/> Service Disabled Veteran <input type="checkbox"/> African American <input type="checkbox"/> Hispanic American <input type="checkbox"/> Pacific Islander American <input checked="" type="checkbox"/> Women-Owned				
AR Certification #: _____		* See <i>Minority and Women-Owned Business Policy</i>			

PROSPECTIVE CONTRACTOR CONTACT INFORMATION			
<i>Provide contact information to be used for bid solicitation related matters.</i>			
Contact Person:	Carolyn Rains	Title:	President
Phone:	601-724-7826	Alternate Phone:	601-594-6060
Email:	crains@fingerpro.net		

CONFIRMATION OF REDACTED COPY
<input type="checkbox"/> YES, a redacted copy of submission documents is enclosed. <input checked="" 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 Bid Solicitation for additional information.</i>
ILLEGAL IMMIGRANT CONFIRMATION
By signing and submitting a response to this <i>Bid Solicitation</i> , a Prospective Contractor agrees and certifies that they do not employ or contract with illegal immigrants. If selected, the Prospective Contractor certifies that they will not employ or contract with illegal immigrants during the aggregate term of a contract.
ISRAEL BOYCOTT RESTRICTION CONFIRMATION
By checking the box below, a Prospective Contractor agrees and certifies that they do not boycott Israel, and if selected, will not boycott Israel during the aggregate term of the contract. <input checked="" type="checkbox"/> Prospective Contractor does not and will not boycott Israel.

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

The signature below signifies agreement that any exception that conflicts with a Requirement of this *Bid Solicitation* will cause the Prospective Contractor's bid to be disqualified:

Authorized Signature: Carolyn Rains Title: President
Use Ink Only.

Printed/Typed Name: Carolyn Rains Date: 03/04/2020

SECTION 1 - VENDOR AGREEMENT AND COMPLIANCE

Any requested exceptions to items in this section which are NON-mandatory **must** be declared below or as an attachment to this page. Vendor **must** clearly explain the requested exception, and should label the request to reference the specific solicitation item number to which the exception applies.

- Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.


Vendor Name:	Automation Designs & Solutions, Inc. d/b/a AD&S, Inc.	Date:	03/04/2020
Signature:	Carolyn Rains	Title:	President
Printed Name:	Carolyn Rains		

SECTION 2 - VENDOR AGREEMENT AND COMPLIANCE

Any requested exceptions to items in this section which are NON-mandatory **must** be declared below or as an attachment to this page. Vendor **must** clearly explain the requested exception, and should label the request to reference the specific solicitation item number to which the exception applies.

- Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.


By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Automation Designs & Solutions, Inc. d/b/a AD&S, Inc.	Date:	03/04/2020
Signature:		Title:	President
Printed Name:	Carolyn Rains		

SECTION 3 - VENDOR AGREEMENT AND COMPLIANCE

Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.


By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Automation Designs & Solutions, Inc. d/b/a AD&S, Inc.	Date:	03/04/2020
Signature:		Title:	President
Printed Name:	Carolyn Rains		

SECTION 4 - VENDOR AGREEMENT AND COMPLIANCE

Exceptions to Requirements **shall** cause the vendor's proposal to be disqualified.

By signature below, vendor agrees to and **shall** fully comply with all Requirements as shown in this section of the bid solicitation.

Vendor Name:	Automation Designs & Solutions, Inc. d/b/a AD&S, Inc.	Date:	03/04/2020
Signature:		Title:	President
Printed Name:	Carolyn Rains		

PROPOSED SUBCONTRACTORS FORM

- **Do not** include additional information relating to subcontractors on this form or as an attachment to this form.


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

**~~X~~ PROSPECTIVE CONTRACTOR DOES NOT PROPOSE TO USE SUBCONTRACTORS TO
PERFORM SERVICES.**

By signature below, vendor agrees to and **shall** fully comply with all Requirements related to subcontractors as shown in the bid solicitation.

Vendor Name:	Automation Designs & Solutions, Inc. d/b/a AD&S, Inc.	Date:	03/04/2020
Signature:		Title:	President
Printed Name:	Carolyn Rains		

State of Arkansas
DEPARTMENT OF HUMAN SERVICES
700 South Main Street
P.O. Box 1437 / Slot W345
Little Rock, AR 72203

ADDENDUM 1

TO: All Addressed Vendors
FROM: Chorsie Burns, Buyer
DATE: March 2, 2020
SUBJECT: 710-20-0026 LIVE SCAN FINGERPRINT CONFIGURATION

The following change(s) to the above referenced IFB have been made as designated below:

- ☒ Change of specification(s)
☐ Additional specification(s)
☐ Change of bid opening date and time
☐ Cancellation of bid
☐ Other-

CHANGE OF SPECIFICATION

Delete item 2.6 (A) 15 which reads as follows:

15. The Fingerprint Configuration **must** have the ability to bill any fees directly to DHS or require payment at time of fingerprint capture.

The specifications by virtue of this addendum become a permanent addition to the above referenced IFB. Failure to return this signed addendum may result in rejection of your proposal.

If you have any questions, please contact Chorsie Burns at chorsie.burns@dhs.arkansas.gov or (501) 682-6327.


Vendor Signature

03/04/2020
Date

Automation Designs & Solutions, Inc. d/b/a AD&S, Inc.
Company

Requirement Group	Requirement Subgroup	Requirement
Application Hosting	Change/Release Management	Any technology vendor, application or solution shall adhere to the Information Technology Infrastructure Library (ITIL) V3.0 Change and Release Management processes.
Application Hosting	Change/Release Management	Any technology vendor, application or solution shall identify and submit any changes in compliance with the DHS Enterprise Program Change/Release Management process.
Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall maintain a detailed Disaster Recovery plan to meet Disaster Recovery requirements. Plan shall include plans for data, back-ups, storage management, and contingency operations that provides for recovering the DHS Enterprise Platform within established recovery requirement timeframes after a disaster that has affected the users of the DHS Enterprise Platform.
Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall provide support to the DHS support teams with implementing, configuring and testing disaster recovery.
Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall develop action plans to address any issues arising from Disaster Recovery testing.
Application Hosting	Infrastructure Security	Any technology vendor, application or solution using cloud technology shall be located within the continental US. All servers and data will be located in US Soil.
Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall proactively monitor all infrastructure including but not limited to network, storage, virtual environments, servers, databases, firewalls, etc. following industry best practices.
Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall implement physical and logical security within new functionality defined in the security plan consistent with DHS' security policies and industry standards.
Application Hosting	Infrastructure Security	Any technology vendor, application or solution shall review all available infrastructure security patches relevant to the environment and classify the need and speed in which the security patches should be installed as defined by DHS security policies.

Application Hosting	Network, Hosting and Data Center Services	Any technology vendor, application or solution shall provision new environments and capacity as required to ensure performance requirements are met as volume increases and additional functionality is implemented.
Application Hosting	Operating System, Application and Database Backup and Recovery	Any technology vendor, application or solution shall encrypt all data at rest including backups using DHS and regulatory bodies (CMS, FNS, etc.) standards regardless of storage media.
Application Hosting	System Monitoring	Any technology vendor, application or solution shall manage and maintain monitoring procedures and standards for system/solution/infrastructure including, but not limited to: a. Monitoring of buffers, database buffers, table space fragmentation, database space, for unusual growth and propose a solution in case of alert b. Monitoring of system logs, update error, database corruption, jobs execution failures etc. and propose solution in case of an alert c. Monitoring of alert notification interface (e.g., Simple Mail Transfer Protocol (SMTP), send mail), and propose a solution in case of an alert d. Monitoring of transaction and trace logs, network event logs and traces, garbage collector, memory and CPU utilization, indexes, etc., and propose a solution in case of an alert e. Monitoring of middleware (e.g., workflows, in- and out-bound queues) and report to DHS according to agreed procedure f. Monitoring and reporting of end-to-end transaction response time to allow measurements against SLAs g. Monitoring of interfaces h. Monitoring of batch jobs and job scheduling
Application Hosting	System Monitoring	Any technology vendor, application or solution shall monitor infrastructure for availability as well as transaction and response time performance.
Application Hosting	System Monitoring	Any technology vendor, application or solution shall provide regular monitoring reports of infrastructure performance, utilization and efficiency (e.g., proactive system monitoring)
Application M&O Services	Disaster Recovery	Any technology vendor, application or solution shall identify and make available appropriate resources to support DHS' disaster recovery planning, testing and execution.

Application M&O Services	Security Administration	Any technology vendor, application or solution shall provide documented procedures for security monitoring and log management functions, and use write-once technology or other secure approaches for storing audit trails and security logs.
Data Governance		
General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall maintain a record (e.g. audit trail) of all additions, changes and deletions made to data in the applicable system or solution. In addition, a log of query or view access to certain type of records and/or screens will be maintained for investigative purposes. This should be readily searchable by user ID or client ID. This must include, but is not limited to: <ul style="list-style-type: none"> a. The user ID of the person who made the change b. The date and time of the change c. The physical, software/hardware and network location (IP address) of the person while making the change d. The information that was changed e. The outcome of the event f. The data before and after it was changed, and which screens were accessed and used
General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall prevent modifications to the audit records.

General System Behavior	Audit_&_Compliance	Any technology vendor, application or solution shall be able to detect security-relevant events (as defined in NIST 800-53 moderate baseline, rev 4) that it mediates and generate audit records for them. At a minimum the events will include, but not be limited to: a. Start/stop b. User login/logout c. Session timeout d. Account lockout e. Client record created/viewed/updated/deleted f. Scheduling g. Query h. Order i. Node-authentication failure j. Signature created/validated k. Personally Identifiable Information (PII) export l. PII import m. Security administration events n. Backup and restore o. Audit Event Types listed in IRS 1075
General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution interfaces will secure and protect (encrypt) the data and the associated infrastructure from a confidentiality, integrity and availability perspective.
General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall develop/integrate services using standardized Web Services formats.
General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution WSDLs developed for Arkansas will conform to the W3C standards for restful API development.
General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution design will allow for the solution to continue to operate despite failure or unavailability of one or more individual technology solution components.

General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the ability to use standards-based communication protocols, such as TCP/IP, HTTP, HTTP/S and SMTP. Protocol bridging: The ability to convert between the protocol native to the messaging platform and other protocols, such as Remote Method Invocation (RMI), IIOP and .NET remoting.
General System Behavior	Perf. and Avail.	Any technology vendor, application or solution must be designed so all releases can be performed between 7pm and 6am except critical releases
General System Behavior	Perf. and Avail.	Any technology vendor, application or solution will provide at least one (1) production and one (1) non-production environment. Highly available solutions that mitigate single points of failure are recommended and encouraged.

General System Behavior	Regulatory_&_Security	<p>Any technology vendor, application or solution shall, at a minimum, provide a mechanism to comply with security requirements and safeguard requirements of the following Federal agencies / entities:</p> <ul style="list-style-type: none"> a. Health & Human Services (HHS) Centers for Medicare & Medicaid Services (CMS) b. Guidance from CMS including MITA Framework 3.0 and Harmonized Security and Privacy Framework c. Administration for Children & Families (ACF) d. Dept. of Agriculture Food and Nutrition Services e. NIST 800-53 r4, MARS-E and DOD 8500.2 f. IRS pub 1075, which points back to NIST 800-53 rev 3 g. Federal Information Security Management Act (FISMA) of 2002 h. Health Insurance Portability and Accountability Act (HIPAA) of 1996 i. Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 j. Privacy Act of 1974 k. e-Government Act of 2002 l. Patient Protection and Affordable Care Act of 2010, Section 1561 Recommendations m. Section 471(a)(8) of the Social Security Act n. Section 106(b)(2)(B)(viii) of the Child Abuse Prevention and Treatment Act
General System Behavior	Regulatory_&_Security	<p>Any technology vendor, application or solution shall adhere to the accessibility standard as outlined in the web guidelines and based on the W3C level 2 accessibility guidelines:</p> <p>(http://www.w3.org/TR/WCAG10/full-checklist.html)</p>
General System Behavior	Regulatory_&_Security	<p>Any technology vendor, application or solution shall adhere to the accessibility standard as outlined in the Section 508 compliance guidelines:</p> <p>(https://www.section508.gov/)</p>
General System Behavior	Regulatory_&_Security	<p>Any technology vendor, application or solution comply with the DHS branding standards as defined by DHS.</p>
General System Behavior	Regulatory_&_Security	<p>Any technology vendor, application or solution shall adhere to the principle of “Fail Safe” to ensure that a system in a failed state does not reveal any sensitive information or leave any access controls open for attacks</p>

General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information
General System Behavior	Regulatory_&_Security	<p>Any technology vendor, application or solution shall follow the DHS Enterprise Architecture Standards regarding identity, authorization and access management.</p> <p>The current standards state that applications/solutions will integrate with Microsoft's Active Directory for internal/DHS users and will integrate with the IBM Cloud Identity platform for external users. Modern authentication protocols such as SAML or OIDC should be used and multi-factor authentication will be employed whenever deemed necessary by DHS or applicable regulatory bodies (CMS, FNS, IRS, etc.).</p>
General System Behavior	Regulatory_&_Security	<p>Any technology vendor, application or solution shall support protection of confidentiality of all Protected Health Information (PHI) and Personally Identifiable Information (PII) delivered over the Internet or other known open networks via supported encryption technologies needed to meet CMS and NIST requirements for encryption of PHI and PII data.</p> <p>Examples include: Advanced Encryption Standard (AES) and an open protocol such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), Internet Protocol Security (IPsec), XML encryptions, or Secure/Multipurpose Internet Mail Extensions (S/MIME) or their successors. All vendors, applications and solutions will be subject to external Audit checks.</p>
General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall, when storing PHI/PII, support the use of encryption technologies needed to meet CMS and NIST requirements for the encryption of PHI/PII data at rest.

General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution, prior to accessing any PHI, display a State-approved configurable warning or login banner (e.g. "The System should only be accessed by authorized users"). In the event that a application or solution does not support pre-login capabilities, the application or solution will display the banner immediately following authorization.
General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall not transmit or store any Personal Health Information (PHI) or Personally Identifiable Information (PII) using publicly available storage over the Internet or any wireless communication device, unless: 1) the PHI or PII is "de-identified" in accordance with 45 C.F.R § 164.514(b) (2); or 2) encrypted in accordance with applicable law, including the American Recovery and Reinvestment Act of 2009 and as required by policies, procedures and standards established by DHS
General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution will include the same security provisions for the development, System test, Acceptance test and training environment as those used in the production environment except those provisions implemented specifically to protect confidential information (e.g. PHI, PII).
General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall be able to associate permissions with a user using one or more of the following access controls: a. Role-Based Access Controls (RBAC; users are grouped by role and access rights assigned to these groups) b. Context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation-location, emergency-mode, etc.)
General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution will comply with accessibility requirements described in 45 CFR 85 and with State of Arkansas accessibility requirements
General System Behavior	Solution Administration	Any technology vendor, application or solution will allow System administrators to create and manage user roles.
General System Behavior	Solution Administration	Any technology vendor, application or solution communications will be protected by at least 256-bit encryption.

General System Behavior	Solution Administration	Any technology vendor, application or solution will be supported by public key/private key encryption Secure Socket Layer (SSL) certificates.
General System Behavior	Usability	Any application or solution will use colors to enhance user experience and System usability while complying with all disability requirements notated elsewhere in these requirements.
General System Behavior	Usability	Any technology vendor, application or solution shall accommodate diverse populations of users including those with disabilities as per State and Federal regulations under the Rehabilitation Act of 1973. The system must be independently verified to be compliant with these regulations. Refer https://www.section508.gov/manage/laws-and-policies
General System Behavior	User Interface	Any technology vendor, application or solution must perform standard data validations such as character, numeric, date, currency , phone, SSN etc.
General System Behavior	User Interface	Any technology vendor, application or solution shall have the ability to create prompts for user actions. (e.g., incomplete data entry of required fields, deletion of data, system log-off warnings).
General System Behavior	User Interface	Any technology vendor, application or solution shall have the capability to send notifications. Examples include sending emails, text messages (SMS), etc.
General System Behavior	Web based UI	Any technology vendor, application or solution providing data over a web browser interface (http, ftp, etc.) will include the capability to encrypt the data communicated over the network via SSL (e.g. HTML over HTTPS).
General System Behavior	Web based UI	The system will support and maintain compatibility with the current to (N-2) version of the DHS Support Operating Systems. The supported Operating Systems are Microsoft Windows, MAC OS, Apple IOS and Google Android.
General System Behavior	Web based UI	The system will support and maintain compatibility with the current to (N-2) version of the DHS approved Browsers. The supported Browsers are Chrome, Edge, and Safari. This is to ensure that vendors test and certify their software/application for current to (N-2) versions of these Browsers.

Meets	Describe How Requirements Met
Yes	Updates are clearly categorized and manually pushed
Yes	
Yes	
Yes	Support is available by phone and/or remote support software
Yes	
Yes	We do not use cloud technology
No	Software does monitor scanning hardware provided by AD&S. Other aspects of infrastructure are outside of scanning software scope
Yes	We use Microsoft BitLocker to provide encryption for the hard drive. The install location is responsible for physical security of the device.
Yes	We typically set the system to install Windows Security Updates when received. Any security patches required outside of window update will be installed by our tech support team.

Yes	These are stand-alone systems. This does not seem to apply. Adequate hard drive space will be defined for DHS.
Yes	We use Microsoft BitLocker to provide encryption for the hard drive.
No	We do not currently offer proactive monitoring
No	
Yes	
Yes	

Yes	Audit logs are stored in the database
Yes	Software maintains an audit trail that includes the user id, date/time, and broad description of what was changed. It does not record before/after values in most cases. Software provides view only access to the audit data.
Yes	Software provides view only access to the audit data.

Yes	Software logs successful/unsuccessful user logins, record created/updated/deleted/replicated events. Scheduling, Query, Order, PII export does not apply to this software. This software does not access Federal Tax Information.
Yes	We use Microsoft BitLocker to provide encryption for the hard drive.
Yes	Software uses a Windows Communication Foundation (WCF) service for invoicing.
Yes	This should not apply but if WSDLs are developed, we will comply.
Yes	Each system is a stand-alone system.

Yes	Our software uses TCP/IP, HTTP, HTTPS, and SMTP. We do not use RMI, IIOP or .NET Remoting.
Yes	Releases can be installed at any time. To comply with CJIS regulations, our access to the system must be observed by an authorized employee which will determine when installation can occur.
Yes	

Yes	We will comply with CJIS regulations.
Yes	Since taking fingerprints requires a visual observation, accessibility is limited in that regard.
Yes	VPAT available
Yes	
Yes	

Yes	Software complies with CJIS regulations.
Yes	We will follow
Yes	Software has no access to PHI. PII is transmitted to Arkansas State Police via sftp using their required encryption.
Yes	We use Microsoft BitLocker to provide encryption for the hard drive.

Yes	This will be implemented via the Windows banner page.
Yes	Data is stored locally on the computer. Backups will be encrypted and transmitted to DHS designated storage if requested.
Yes	We will comply.
Yes	Software uses Role-Based Access Control.
Yes	Program is accessible to visually-impaired and no audio component is required
Yes	Software complies
Yes	Software complies

Yes	
Yes	Software complies.
Yes	Software complies
Yes	Software complies.
Yes	We prompt for data that does not pass validation and to confirm deletions.
Yes	Email and creations can be sent if appropriate infrastructure is available
Yes	We use SFTP and HTTPS
No	Software is Microsoft Windows only. Currently we support Windows 10. Development availability soon for android/ios
Yes	Software does not use a web browser.

Equal Employment Opportunity

APPROVED BY: Carolyn Rains

EFFECTIVE DATE: September 1, 2005

LAST REVISION: January 1, 2020

Purpose:

To state the commitment of the system to Equal Employment Opportunity.

Policy:

1. Automation Designs & Solutions, Inc. d/b/a AD&S, Inc. is an equal opportunity employer. No person is unlawfully excluded from consideration for employment because of race, color, religious creed, national origin, ancestry, sex, age, veteran status, marital status or physical challenges.
2. The policy applies not only to recruitment and hiring practices, but also includes affirmative action in the area of placement, promotion, transfer, rate of pay and termination.
3. Management has the responsibility to further the implementation of this policy and ensure conformance by subordinates.
4. Any AD&S Company employee who engages in discrimination will be subject to suspension or termination.
5. Any supervisory or managerial employee who knows of such behavior and fails to take immediate and appropriate corrective action will also be subject to disciplinary action.
6. Any individual who is the target of discrimination is encouraged to discuss the matter with the Department Director.
7. Any individual who feels such a discussion would be or has been futile, unsatisfactory or counterproductive should contact Management.
8. Management will investigate the claim.
9. The accused individual may be suspended pending the outcome of the investigation.
10. Retaliation against claimants will not be tolerated.

AD&S is proud to be an equal opportunity employer. We are committed to providing equal employment opportunities to all persons without regard to race, creed, color, religion, national origin, sex, marital status, citizenship status, age, veteran status or disability.

Furthermore, we will not tolerate any form of discrimination or harassment of our employees by co-workers, supervisors, customers, or vendors. This commitment extends to our policies on recruiting, advertising, hiring, placement, promotion, training, transfer, wages, benefits, termination and all other privileges, terms and conditions of employment.

Contract Number _____
Attachment Number _____
Action Number _____

CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM

Failure to complete all of the following information may result in a delay in obtaining a contract, lease, purchase agreement, or grant award with any Arkansas State Agency.

SUBCONTRACTOR: SUBCONTRACTOR NAME:

☐ Yes ☒ No

IS THIS FOR:

TAXPAYER ID NAME: 64-0770610

Goods? ☐ Services? ☒ Both? ☐

YOUR LAST NAME: Rains

FIRST NAME Carolyn

M.I.:

ADDRESS: 1070 lake Village Circle, Suite D

CITY: Brandon

STATE: MS

ZIP CODE: 39047

COUNTRY: US

AS A CONDITION OF OBTAINING, EXTENDING, AMENDING, OR RENEWING A CONTRACT, LEASE, PURCHASE AGREEMENT, OR GRANT AWARD WITH ANY ARKANSAS STATE AGENCY, THE FOLLOWING INFORMATION MUST BE DISCLOSED:

FOR INDIVIDUALS *

Indicate below if: you, your spouse or the brother, sister, parent, or child of you or your spouse is a current or former: member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee:

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/ commission, data entry, etc.]	For How Long?		What is the person(s) name and how are they related to you? [i.e., Jane Q. Public, spouse, John Q. Public, Jr., child, etc.]	
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Relation
General Assembly							
Constitutional Officer							
State Board or Commission Member							
State Employee							

☐ None of the above applies

FOR AN ENTITY (BUSINESS) *

Indicate below if any of the following persons, current or former, hold any position of control or hold any ownership interest of 10% or greater in the entity: member of the General Assembly, Constitutional Officer, State Board or Commission Member, State Employee, or the spouse, brother, sister, parent, or child of a member of the General Assembly, Constitutional Officer, State Board or Commission Member, or State Employee. Position of control means the power to direct the purchasing policies or influence the management of the entity.

Position Held	Mark (√)		Name of Position of Job Held [senator, representative, name of board/commission, data entry, etc.]	For How Long?		What is the person(s) name and what is his/her % of ownership interest and/or what is his/her position of control?		
	Current	Former		From MM/YY	To MM/YY	Person's Name(s)	Ownership Interest (%)	Position of Control
General Assembly								
Constitutional Officer								
State Board or Commission Member								
State Employee								

☒ None of the above applies

Contract Number _____
Attachment Number _____
Action Number _____

Contract and Grant Disclosure and Certification Form

Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this contract. Any contractor, whether an individual or entity, who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the agency.

As an additional condition of obtaining, extending, amending, or renewing a contract with a state agency I agree as follows:

1. Prior to entering into any agreement with any subcontractor, prior or subsequent to the contract date, I will require the subcontractor to complete a **CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM**. Subcontractor shall mean any person or entity with whom I enter an agreement whereby I assign or otherwise delegate to the person or entity, for consideration, all, or any part, of the performance required of me under the terms of my contract with the state agency.
2. I will include the following language as a part of any agreement with a subcontractor:

Failure to make any disclosure required by Governor's Executive Order 98-04, or any violation of any rule, regulation, or policy adopted pursuant to that Order, shall be a material breach of the terms of this subcontract. The party who fails to make the required disclosure or who violates any rule, regulation, or policy shall be subject to all legal remedies available to the contractor.
3. No later than ten (10) days after entering into any agreement with a subcontractor, whether prior or subsequent to the contract date, I will mail a copy of the **CONTRACT AND GRANT DISCLOSURE AND CERTIFICATION FORM** completed by the subcontractor and a statement containing the dollar amount of the subcontract to the state agency.

I certify under penalty of perjury, to the best of my knowledge and belief, all of the above information is true and correct and that I agree to the subcontractor disclosure conditions stated herein.

Signature Carolyn Rains Title President Date 03/04/2020
Vendor Contact Person Carolyn Rains Title President Phone No. (601) 724-7826

Agency use only

Agency Number 0710 Agency Name Department of Human Services Agency Contact Person _____ Contact Phone No. _____ Contract or Grant No. _____



Rankin County School District

TRADITION OF EXCELLENCE

BRANDON FLORENCE MCLAURIN NORTHWEST PELAHATCHIE PISGAH PUCKETT RICHLAND

Post Office Box 1359 | Brandon, MS 39043 | p 601.825.5590 | f 601.825.2618 | www.rcsd.ms

March 5, 2020

Dear Mr. Burns,

On behalf of the RCSD, I highly recommend the services and products provided by Automation Designs & Solutions, Inc d/b/a AD&S, Inc. I am the main user and contact for our school district for FingerPro ID system located in Flowood, MS. The first system was purchased in 2016 and the second system was purchased in 2017. I was not in this position at the time of implementation of this product and service but have been thoroughly trained to use this product and service. The RCSD has 2 standalone fingerprint capture and transmission systems from AD&S, Inc. AD&S has been excellent in training me and other new staff on FingerPro ID. FingerPro ID has been easy to learn and navigate. AD&S is quick to respond to any issue that we may have. AD&S provides excellent support remotely which allows problems to be resolved quickly. We have been thoroughly pleased with this product and service. If you have any questions, feel free to contact me.

Sincerely,

Michelle Morris

michelle.morris@rcsd.ms

Human Resource Administrative Assistant

Rankin County School District

1220 Apple Park Place

Brandon, MS 39042

601-825-5590 ext. 1060

Dr. Sue Townsend

Superintendent of Education



March 5, 2020

To Whom It May Concern:

It is with much enthusiasm that I am writing to recommend the services and products provided by Automation Designs & Solutions, Inc d/b/a AD&S, Inc. I am one of the main users for our FingerPro ID system located in Flowood, MS. I was also the main contact for installation of all FingerPro ID systems and onsite training for all locations.

In September of 2017, Sta-Home Health purchased seven (7) standalone fingerprint capture and transmission systems from AD&S, Inc. AD&S, Inc installed our systems in October 2017. The technicians provided a detailed onsite training session for our device coordinators. AD&S, Inc. has responded to any issue we have had with the system quickly and efficiently. They provide support remotely and this has allowed us to have any problems resolved almost immediately.

FingerPro ID has been easy for us coordinators to learn. It is so convenient to be able to take the fingerprints, transmit and get results timely.

I am happy to recommend AD&S, Inc. to provide FingerPro ID transmission systems. If you have any questions, please feel free to contact me.

Sincerely,

A handwritten signature in black ink, appearing to read 'Faye Dunaway', with a stylized flourish at the end.

Faye Dunaway | Regional Office Coordinator

Office: 601.899.1496 Ext 8177

Cell: 601.209.4822

Fax: 601.956.4782

Email: ldunaway@sta-home.com