

Health Management Systems, Inc., a Gainwell Technologies
Company Response to

Arkansas Department of Human Services for **Asset Verification Services**

IFB 710-23-0052



Invitation for Bid Response

REDACTED VERSION

July 26, 2023

1:00 p.m. CST

Confidential

gainwell
HMS, a Gainwell Technologies Company

Table of Contents

Bid Signature Page	2
Sections 1 – 4: Vendor Agreement and Compliance	3
Proposed Subcontractors Form	4
EO 98-04 Disclosure Form (Attachment A)	5
Equal Opportunity Policy	6
Signed Addenda.....	7
Minimum Qualifications	9
Certificate of Good Standing	10
Licensure and Certification Documents	11
Financial Institutions	18
CMS Asset Verification Program Experience.....	106
References.....	107
Letter of Bondability	108
Attachment H: IT Requirements	109

BID SIGNATURE PAGE

Type or Print the following information.

PROSPECTIVE CONTRACTOR'S INFORMATION				
Company:	Health Management Systems, Inc. (HMS)			
Address:	5615 High Point Drive			
City:	Irving	State: TX		Zip Code: 75038
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 checked="" 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 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 bid solicitation related matters.</i>			
Contact Person:	Bonnie Vaughn	Title:	Sr. Dir. of Business Development
Phone:	512.660.9870	Alternate Phone:	404.290.2020
Email:	bonnie.vaughn@gainwelltechnologies.com		

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 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:

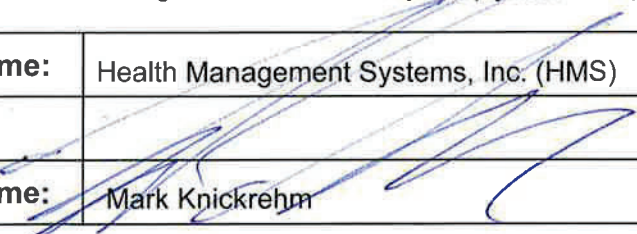
Authorized Signature:  **Title:** Chief Executive Officer
Printed/Typed Name: Mark Knickrehm **Date:** July 26, 2023

SECTIONS 1 - 4 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.

HMS requests no exceptions to items in these sections.

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

Vendor Name:	Health Management Systems, Inc. (HMS)	Date:	July 26, 2023
Signature:		Title:	Chief Executive Officer
Printed Name:	Mark Knickrehm		


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
Accuity Asset Verification Services, Inc.	1007 Church Street, Suite 600	Evanston, Illinois, 60201



Mark Knickrehm, Chief Executive Officer

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

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: Health Management Systems, Inc. (HMS)

Goods? ☐ Services? ☒ Both? ☐

YOUR LAST NAME:

FIRST NAME

M.I.:

ADDRESS: 5615 High Point Drive

CITY: Irving

STATE:

TX

ZIP CODE: 75038

COUNTRY: USA

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.]	Person's Name(s)	Relation
	Current	Former		From MM/YY	To MM/YY			
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 position of control? what is his/her position of control?	Ownership Interest (%)	Position of Control
	Current	Former		From MM/YY	To MM/YY			
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 _____

Title Chief Executive Officer

Date July 26, 2023

Vendor Contact Person Bonnie Vaughn

Title Senior Director of Business Development

Phone No. (512) 660-9870

Agency use only

Agency Number 0710

Agency Name Department of Human Services

Agency Contact Person

Contact Phone No.

Contract or Grant No.

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 NAME: _____

☐ Yes ☒ No

Account Asset Verification Services Inc

IS THIS FOR:

TAXPAYER ID NAME: _____

46-1451339

Goods? ☐ Services? ☒ Both? ☐

YOUR LAST NAME: _____

Balaban

FIRST NAME

Tyson

M.I.: _____

ADDRESS: _____

1007 Church St, Suite 600

CITY: _____

Evansston

STATE: _____

IL

ZIP CODE: _____

60201

COUNTRY: _____

USA

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.]	Relation
	Current	Former		From MM/YY	To MM/YY		
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?	Ownership Interest (%)	Position of Control
	Current	Former		From MM/YY	To MM/YY			
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 Juan Belar Title Sales Director Date 7/12/2023
Vendor Contact Person Sason Balaban Title Sales Director Phone No. 214/2023

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

Equal Opportunity Policy

Employees deserve to work in an environment where they are treated with dignity and respect. Gainwell is committed to creating such an environment because it brings out the full potential in each of us, which, in turn, contributes directly to our business success. We cannot afford to let anyone's talents go to waste. Gainwell is an equal employment opportunity employer and is committed to providing a workplace that is free of forms of unlawful harassment, discrimination, and retaliation by supervisors, managers, co-workers, or third parties.

If you feel you have witnessed or been subjected to unlawful harassment, discrimination, or retaliation, report it to your manager or to Human Resources. You may also report it anonymously through the Gainwell Hotline at www.gainwelltechnologies.ethicspoint.com or by calling 833.331.1349.

Gainwell employees are also expected to support an inclusive workplace by adhering to the following conduct standards:

- Treat others with dignity and respect at all times.
- Address and report inappropriate behavior and comments that are discriminatory, harassing, abusive, offensive, or unwelcome.
- Foster teamwork and employee participation, encouraging the representation of different employee perspectives.
- Seek out insights from employees with different experiences, perspectives, and backgrounds. Avoid slang or idioms that might not translate across cultures.
- Support flexible work arrangements for co-workers with different needs, abilities and/or obligations. Confront the decisions or behaviors of others that are based on conscious or unconscious biases.
- Be open-minded and listen when given constructive feedback regarding others' perception of your conduct.

Gainwell will not tolerate unlawful harassment, discrimination, retaliation, behavior, or language that is abusive, offensive, or unwelcome.

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: Office of Procurement
DATE: June 29, 2023
SUBJECT: 710-23-0052 Asset Verification Services

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

OTHER

- Change Buyer's direct phone number to the following: Buyer's Direct Phone Number: **501-683-6456**

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: Buyer's name, Buyer's email address and phone number.

Vendor Signature

Health Management Systems, Inc. (HMS)

Company

July 26, 2023

Date

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

ADDENDUM 2

TO: All Addressed Vendors
FROM: Office of Procurement
DATE: July 12, 2023
SUBJECT: 710-23-0052 Asset Verification Services

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 SPECIFICATIONS

- **Section 2.18 of the solicitation – remove and replace with the following:**
The Contractor shall provide technical support to DHS and FI staff. The Contractor must provide support and shall be available during DHS normal business hours Monday through Friday, except State holidays (8:00 am – 4:30 pm central time). Calls received after normal business hours must have the option to leave a voice message. Voice messages must be returned the next business day.

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: Buyer's name, Buyer's email address and phone number.

Vendor Signature

Health Management Systems, Inc. (HMS)

Company

July 26, 2023

Date

Minimum Qualifications

MINIMUM QUALIFICATIONS: The Contractor must meet the following requirements:

- A. The Contractor must be registered to do business in the State of Arkansas and in good standing by the initial start of any resulting contract. For verification purposes, Contractor must provide a Certificate of Good Standing, Certificate of Authority, other required Arkansas Secretary of State documentation such as non-filing or nonqualifying statements, upon DHS request.
- B. The bidder must include a copy of all required licensure and certification documents in the bidder's response to this solicitation. See "Response Documents."
- C. The Contractor shall have an established network of Financial Institutions (FIs) who will participate in the AVS. For verification purposes, Prospective Contractor must provide a listing of FIs with bid submission and describe the methodology for securing additional FIs.
- D. The Contractor must have experience within the last five (5) years in CMS asset verification programs. For verification purposes, the Prospective Contractor must provide three (3) references from entities to which the Prospective Contractor has provided financial AVS. Each reference should include the entity's name, summary of program, dates, name, mailing address, telephone number, and email address of the individual with knowledge of the work provided.
- E. The Contractor must be bondable. For verification purposes the Prospective Contractor must submit a Letter of Bondability from an admitted Surety Insurer with bid submission. The letter must unconditionally offer to guarantee, to the extent of one hundred percent (100%) of the annual contract price, the Prospective Contractor's performance in all respects of the terms and conditions of the IFB and the resultant contract. The Prospective Contractor shall be required to provide DHS with the Performance Bond described in this section upon contract start.

HMS confirms our ability to meet the minimum qualifications listed in Section 2.2 of the RFP and have included in our proposal response a copy of the items listed in the documentation checklist of the solicitation package.

HMS understands that the Arkansas Department of Health Services (DHS) has a fiscal responsibility to validate assets held at various Financial Institutions (FIs) by Medicaid applicants and beneficiaries. As states seek to improve the quality of the services they provide to their citizens, modernizing their asset verification system has become a necessary step in the journey. As a current asset verification solution provider to the Arkansas DHS, HMS is poised to continue meet DHS' goals.



**Arkansas Secretary of State
John Thurston**

State Capitol Building ♦ Little Rock, Arkansas 72201-1094 ♦ 501-682-3409

Certificate of Good Standing

I, John Thurston, Secretary of State of the State of Arkansas, and as such, keeper of the records of domestic and foreign corporations, do hereby certify that the records of this office show

THIRD PARTY LIABILITY RECOVERY

formed under the laws of the state of New York, and authorized to transact business in the State of Arkansas as a Foreign For Profit Corporation, was granted a Application for Certificate of Authority by this office September 23, 1994.

Our records reflect that said entity, having complied with all statutory requirements in the State of Arkansas, is qualified to transact business in this State.



In Testimony Whereof, I have hereunto set my hand and affixed my official Seal. Done at my office in the City of Little Rock, this 5th day of July 2023.


John Thurston

Secretary of State

Online Certificate Authorization Code: 59a5a9f5ecc55d8

To verify the Authorization Code, visit sos.arkansas.gov

Licensure and Certification Documents

FAIR CREDIT REPORTING ACT ADDENDUM TO ATTACHMENT E MASTER TERMS AND CONDITIONS

1. Fair Credit Reporting Act (“FCRA”) Obligations. The Department certifies that when using Contract Services that constitute a Consumer Report as defined by FCRA (the “FCRA Contract Services”), it will comply with all applicable provisions of FCRA (15 U.S.C. § 1681 et seq.) and all other applicable federal, state, and local legislation, regulations, and rules. In addition, the Department certifies it has a permissible purpose under the FCRA for obtaining a Consumer Report and will re-certify such permissible purpose to Contractor upon request. The Department acknowledges that Contractor has provided the “Notice to Users of Consumer Reports”, attached hereto as Attachment 1, which informs users of consumer reports of their legal obligations under the FCRA.

ATTACHMENT 1 TO FAIR CREDIT REPORTING ACT ADDENDUM

All users of consumer reports must comply with all applicable regulations. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau’s website, www.consumerfinance.gov/learnmore.

NOTICE TO USERS OF CONSUMER REPORTS: OBLIGATIONS OF USERS UNDER THE FCRA

The Fair Credit Reporting Act (“FCRA”), 15 U.S.C. § 1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Consumer Financial Protection Bureau’s (“CFPB”) website at www.consumersfinance.gov/learnmore. Other information about user duties is also available at the CFPB’s website. **Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.**

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (“CRA”), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers’ privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 contains a list of the permissible purposes under the law. These are:

- As ordered by a court of federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a)(2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(8) and 604(b)
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)
- For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604(a)(5)

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making “prescreened” unsolicited offers of credit or insurance. Section 604(c). The particular obligations of users of “prescreened” information are described in Section VII below.

B. Users Must Provide Certifications

Section 604(f) prohibits any person from obtaining a consumer report from a CRA unless the person has certified to the CRA the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers when Adverse Actions Are Taken

The term “adverse action” is defined very broadly by Section 603. “Adverse actions” include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact as defined by Section 603(k) of the FCRA – such as denying or canceling credit or insurance or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action as defined by the FCRA that is based at least in part on information contained in a consumer report, Section 615(a) requires the user to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following:

- The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.

- A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
- A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

2. Adverse Actions Based on Information Obtained From Third Parties Who Are Not Consumer Reporting Agencies

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained From Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure as set forth in I.C.1 above.

D. Users Have Obligations When Fraud and Active-Duty Military Alerts are in Files

When a consumer has placed a fraud alert, including one relating to identity theft, or an active-duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active-duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extended fraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the consumer's file. When this occurs,

users must comply with regulations specifying the procedures to be followed. Federal regulations are available at www.consumerfinance.gov/learnmore.

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. Federal regulations have been issued that cover disposal.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

If a person uses a consumer report in connection with an application for, or a grant, extension, or provision of, credit to a consumer on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person, based in whole or in part on a consumer report, the person must provide a risk-based pricing notice to the consumer in accordance with regulations prescribed by the CFPB.

Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) ("Notice to the Home Loan Applicant").

III. OBLIGATIONS OF USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

A. Employment Other Than in the Trucking Industry

If the information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.
- Before taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of consumer's rights (The user should receive this summary from the CRA.) A Section 615(a) adverse action notice should be sent after the adverse action is taken.

An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2).

The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry

Special rules apply for truck drivers where the only interaction between the consumer and the potential employer is by mail, telephone, or computer. In this case, the consumer may provide consent orally or electronically, and an adverse action may be made orally, in writing, or electronically. The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by an entity or person that is a consumer reporting agency. Consumers who are the subjects of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)
- The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure described below.
- Upon the written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with Federal, state, or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long as the employer or its agent complies with the procedures set forth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not

identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report, or the information must be coded. If the report is to be used for employment purposes – or in connection with a credit transaction (except as provided in federal regulations) – the consumer must provide specific written consent and the medical information must be relevant.

Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or a permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF “PRESCREENED” LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(1), 604(c), 604(e), and 615(d). This practice is known as “prescreening” and typically involves obtaining from a CRA a list of consumers who meet certain pre-established criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer.

In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in a consumer’s CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.
- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system.

In addition, the CFPB has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The regulation is 12 CFR 1022.54.

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

Section 607(e) requires any person who obtains a consumer report for resale to take the following steps:

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.

- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:
 - (1) the identity of all end-users.
 - (2) certifications from all users of each purpose for which reports will be used; and
 - (3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

Under Section 611(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CRA for reinvestigation. When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

C. Fraud Alerts and Resellers

Section 605A(f) requires resellers who receive fraud alerts or active-duty alerts from another consumer reporting agency to include these in their reports.

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCRA can result in state government or federal government enforcement actions, as well as private lawsuits. Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Section 619.

The CFPB's website, www.consumerfinance.gov/learnmore, has more information about the FCRA, including publications for businesses and the full text of the FCRA.

Financial Institutions

Our team, comprised of both Gainwell and our subcontractor, Accuity Asset Verification Services, Inc (Accuity), has one of the largest, most-diverse networks of Financial Institutions (FIs) in the market today, both in Arkansas and across the nation, including U.S. possessions and territories. There are 9,971 FIs and more than 101,000 U.S. bank locations already participating in Accuity's network for Asset Verification Services (AVS). For Arkansas' AVS project, Accuity will continue to achieve maximum participation by FIs in Arkansas and its border states as well as throughout the United States through each segment of the depository FI community. The list of FIs currently within our network is included on the following pages.

Accuity's FI network-management plan provides the components and methods used to fulfill this task. The plan has its basis in Accuity's long-standing relationships with the banking industry as the Registrar of American Bankers Association (ABA) routing numbers.

Since 1911, Accuity has held the role of Official Registrar of the ABA routing and transit codes within the U.S. banking system. In this role, the company acts as the issuing body for the ABA routing codes for FIs. As a result, U.S. domiciled banks, savings and loans, credit unions, and deposit taking FIs must provide information to Accuity regarding structural changes in the banking system within the United States. Such changes include mergers, acquisitions, new bank charters, new locations, and closed locations. Accuity has successfully leveraged this unique role to provide a secure network for the direct conveyance of sensitive financial account information between the FI community and the government agencies. Among its hundreds of employees, Accuity has a team of more than 75 Data professionals who communicate with the banking market on a daily basis to update information critical to those operating in the FI community. Accuity averages up to 5,000 updates to the FI Database it maintains for more than 101,000 U.S. bank locations.

Accuity will notify FIs already participating in its FI network that DHS has contracted with it (through HMS) to conduct asset-verification searches. Upon their initial enrollment in the Accuity network for AVS, these FIs agreed to participate in services for additional states. Accuity anticipates that FIs currently in its network will participate in the DHS' AVS project. Accuity personnel will inform these FIs that Accuity will begin to process asset-verification requests for Arkansas based on the work plan we will establish with DHS.

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

[illegible]

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

Health Management Systems, Inc. (a Gainwell Technologies company)

INST ID	FI NAME	HEAD OFFICE CITY	HEAD OFFICE STATE
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

CMS Asset Verification Program Experience

Our team leads the industry in providing Asset Verification Services (AVS) solutions to federal, state, and Medicaid agency clients. HMS has been providing AVS to state and Medicaid agencies since 2012. Our subcontractor, Accuity, has been a leader in AVS for more than 20 years.

Together, HMS and Accuity have combined to provide a robust automated asset verification solution that meets Centers for Medicare & Medicaid Services (CMS) and National Institute of Standards and Technology (NIST) requirements including Section 1940 of the Social Security Act (42 U.S.C §1396w). As the incumbent, we have implemented the asset verification solution for the Arkansas Department of Human Services with Accuity. HMS and Accuity have implemented AVS for the State of South Carolina Department of Health and Human Services. In addition, Accuity AVS software is operational in 46 Medicaid Agencies and Washington, DC.

We take the security and privacy of our State-agency client's information serious which is why we make certain to adhere to local, state, and federal laws and regulations relating to privacy and data security, which includes the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as well as those laws regulating the Protection of Personally Identifiable Information (PII), and Protected Health Information (PHI).

References

Reference 1: [REDACTED]	
Company Name:	[REDACTED]
Contact Name:	[REDACTED]
Address:	[REDACTED]
Phone:	[REDACTED]
Email:	[REDACTED]
Project Start:	[REDACTED]
Project End:	[REDACTED]

Reference 2: Social Security Administration	
Company Name:	[REDACTED]
Contact Name:	[REDACTED]
Address:	[REDACTED]
Phone:	[REDACTED]
Email:	[REDACTED]
Project Start:	[REDACTED]
Project End:	[REDACTED]

Reference 3: State of North Carolina	
Company Name:	[REDACTED]
Contact Name:	[REDACTED]
Address:	[REDACTED]
Phone:	[REDACTED]
Email:	[REDACTED]
Project Start:	[REDACTED]
Project End:	[REDACTED]



Letter of Intent

Obligee: State of Arkansas Department of Human Services

Address: Office of Procurement, 700 Main Street, Slot W345, Little Rock, AR 72201


Re: HMS a Gainwell Technologies Company

Project Name: Asset Verification Services

The Harco National Insurance Company, herein referred to as Surety, a corporation organized and existing under the laws of the State of Illinois and duly authorized to transact business in the State of Arkansas, hereby agrees that if the contract for State of Arkansas Department of Human Services, for which the accompanying proposal is made, be awarded to HMS a Gainwell Technologies Company, the Surety will furnish a performance bond in the amount set forth in the terms of the contract. This letter is not an assumption of liability; the final decision to execute any bond will be subject to the normal underwriting consideration at the time of request.

Signed, sealed, and dated this 7th day of July, 2023.

Harco National Insurance Company

A handwritten signature in cursive script that reads "Terry Ann Gonzales-Selman".

Terry Ann Gonzales-Selman, Attorney-in-Fact



POWER OF ATTORNEY

Bond # NA

HARCO NATIONAL INSURANCE COMPANY INTERNATIONAL FIDELITY INSURANCE COMPANY

Member companies of IAT Insurance Group, Headquartered: 4200 Six Forks Rd, Suite 1400, Raleigh, NC 27609

KNOW ALL MEN BY THESE PRESENTS: That **HARCO NATIONAL INSURANCE COMPANY**, a corporation organized and existing under the laws of the State of Illinois, and **INTERNATIONAL FIDELITY INSURANCE COMPANY**, a corporation organized and existing under the laws of the State of New Jersey, and having their principal offices located respectively in the cities of Rolling Meadows, Illinois and Newark, New Jersey, do hereby constitute and appoint

KELLY O'MALLEY, TERRY ANN GONZALES-SELMAN, ANNETTE AUDINOT, ANTONIO V. CORASANITI, MEGAN J. SCHLUETER, FRANCESCA PAPA, MARIYA LEONIDOV

New York, NY

their true and lawful attorney(s)-in-fact to execute, seal and deliver for and on its behalf as surety, any and all bonds and undertakings, contracts of indemnity and other writings obligatory in the nature thereof, which are or may be allowed, required or permitted by law, statute, rule, regulation, contract or otherwise, and the execution of such instrument(s) in pursuance of these presents, shall be as binding upon the said **HARCO NATIONAL INSURANCE COMPANY** and **INTERNATIONAL FIDELITY INSURANCE COMPANY**, as fully and amply, to all intents and purposes, as if the same had been duly executed and acknowledged by their regularly elected officers at their principal offices.

This Power of Attorney is executed, and may be revoked, pursuant to and by authority of the By-Laws of **HARCO NATIONAL INSURANCE COMPANY** and **INTERNATIONAL FIDELITY INSURANCE COMPANY** and is granted under and by authority of the following resolution adopted by the Board of Directors of **INTERNATIONAL FIDELITY INSURANCE COMPANY** at a meeting duly held on the 13th day of December, 2018 and by the Board of Directors of **HARCO NATIONAL INSURANCE COMPANY** at a meeting held on the 13th day of December, 2018.

"RESOLVED, that (1) the Chief Executive Officer, President, Executive Vice President, Senior Vice President, Vice President, or Secretary of the Corporation shall have the power to appoint, and to revoke the appointments of, Attorneys-in-Fact or agents with power and authority as defined or limited in their respective powers of attorney, and to execute on behalf of the Corporation and affix the Corporation's seal thereto, bonds, undertakings, recognizances, contracts of indemnity and other written obligations in the nature thereof or related thereto; and (2) any such Officers of the Corporation may appoint and revoke the appointments of joint-control custodians, agents for acceptance of process, and Attorneys-in-fact with authority to execute waivers and consents on behalf of the Corporation; and (3) the signature of any such Officer of the Corporation and the Corporation's seal may be affixed by facsimile to any power of attorney or certification given for the execution of any bond, undertaking, recognizance, contract of indemnity or other written obligation in the nature thereof or related thereto, such signature and seals when so used whether heretofore or hereafter, being hereby adopted by the Corporation as the original signature of such officer and the original seal of the Corporation, to be valid and binding upon the Corporation with the same force and effect as though manually affixed."

IN WITNESS WHEREOF, **HARCO NATIONAL INSURANCE COMPANY** and **INTERNATIONAL FIDELITY INSURANCE COMPANY** have each executed and attested these presents on this 31st day of December, 2022



STATE OF NEW JERSEY
County of Essex

Kenneth Chapman

Executive Vice President, Harco National Insurance Company
and International Fidelity Insurance Company

STATE OF ILLINOIS
County of Cook



On this 31st day of December, 2022, before me came the individual who executed the preceding instrument, to me personally known, and, being by me duly sworn, said he is the therein described and authorized officer of **HARCO NATIONAL INSURANCE COMPANY** and **INTERNATIONAL FIDELITY INSURANCE COMPANY**; that the seals affixed to said instrument are the Corporate Seals of said Companies; that the said Corporate Seals and his signature were duly affixed by order of the Boards of Directors of said Companies.



IN TESTIMONY WHEREOF, I have hereunto set my hand affixed my Official Seal, at the City of Newark, New Jersey the day and year first above written.

Cathy Cruz a Notary Public of New Jersey
My Commission Expires April 16, 2024

CERTIFICATION

I, the undersigned officer of **HARCO NATIONAL INSURANCE COMPANY** and **INTERNATIONAL FIDELITY INSURANCE COMPANY** do hereby certify that I have compared the foregoing copy of the Power of Attorney and affidavit, and the copy of the Sections of the By-Laws of said Companies as set forth in said Power of Attorney, with the originals on file in the home office of said companies, and that the same are correct transcripts thereof, and of the whole of the said originals, and that the said Power of Attorney has not been revoked and is now in full force and effect.

IN TESTIMONY WHEREOF, I have hereunto set my hand on this day, July 7, 2023

A02249

Irene Martins, Assistant Secretary

HARCO NATIONAL INSURANCE COMPANY

1701 GOLF ROAD, SUITE 1-600, ROLLING MEADOWS, IL 60008

STATEMENT OF ASSETS, LIABILITIES, SURPLUS AND OTHER FUNDS AT DECEMBER 31, 2022

ASSETS

Bonds (Amortized Value)	\$102,874,915
Stocks (Preferred Stocks)	4,295,218
Stocks (Common Stocks)	814,084,691
Cash, Bank Deposits & Short-Term Investments	60,471,579
Other Invested Assets	8,819,426
Unpaid Premiums & Assumed Balances	137,085,120
Deferred Premiums, Agents Balances & Installments booked	13,474,014
Reinsurance Recoverable from Reinsurers	199,602,884
Reinsurance - Funds Held by or deposited with reinsured companies ..	11,122,630
Current Federal & Foreign Income Tax Recoverable & Interest	970,150
Investment Income Due and Accrued	1,568,572
Receivables from Parent Subsidiaries & Affiliates	14,533,189
Other Assets	1,834,611
TOTAL ASSETS	<u>\$1,370,736,999</u>

LIABILITIES, SURPLUS & OTHER FUNDS

Losses (Reported Losses Net as to Reinsurance Ceded and Incurred But Not Reported Losses)	\$193,234,836
Reinsurance payable on paid losses & loss adjustment expense	19,375,741
Loss Adjustment Expenses	41,894,027
Commissions Payable, Contingent Commissions & Other Similar Charges	6,862,698
Other Expenses (Excluding Taxes, Licenses and Fees)	55,455
Taxes, Licenses & Fees (Excluding Federal Income Tax)	2,087,610
Current federal and foreign income taxes	0
Net Deferred Tax Liability	5,825,659
Unearned Premiums	145,821,961
Advance Premium	570,389
Ceded Reinsurance Premiums Payable	143,069,103
Funds held by Company under reinsurance treaties	14,995,636
Amounts Withheld by Company for Account of Others	50,882,329
Payable to Parent Subsidiaries & Affiliates	4,127,577
Other Liabilities	5,058,571
TOTAL LIABILITIES	<u>\$633,861,592</u>

Common Capital Stock	\$3,500,004
Gross Paid-in & Contributed Surplus	670,781,834
Unassigned Funds (Surplus)	62,593,569
Surplus as Regards Policyholders	<u>\$736,875,407</u>
TOTAL LIABILITIES, SURPLUS & OTHER FUNDS	<u>\$1,370,736,999</u>



I, John Mruk, Treasurer of HARCO NATIONAL INSURANCE COMPANY, certify that the foregoing is a fair statement of Assets, Liabilities, Surplus and Other Funds of this Company, at the close of business, December 31, 2022, as reflected by its books and records and as reported in its statement on file with the Insurance Department of the State of Illinois.

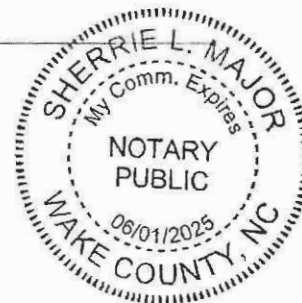
IN TESTIMONY WHEREOF, I have set my hand and affixed the
seal of the Company, this 21st day of March, 2023.
HARCO NATIONAL INSURANCE COMPANY

J. M. Mruk

SIGNED AND SWORN to before me on this 21st day of March, 2023.

NOTARY PUBLIC, STATE OF

Sherrie L. Major
North Carolina





Addendum: Usage of e-Seal and e-Signature for Harco and IFIC Surety Bond Forms

Harco National Insurance Company and International Fidelity Insurance Company (herein the "Company") have authorized our network of surety partners, as granted under the attached Power of Attorney, stipulated within the terms of a signed Agency Agreement and duly appointed by the Company under a Department of Insurance appointment (where required) within all 50 U.S. States, plus U.S. territories and possessions, to affix an electronic e-seal to all bond documents as if it were a raised corporate seal. This addendum also extends to the use of an e-signature by our appointed surety partners authorized under the Company Power of Attorney.

This authority is effective on this day, the 24th of May 2022 and shall remain in place indefinitely unless and until revoked by the Company.

Harco National Insurance Company and International Fidelity Insurance Company



A handwritten signature in black ink, appearing to read 'Kenneth Chapman'.

Authorized by: Kenneth Chapman
Executive Vice President, Surety

Requirement Number	Requirement Group	Requirement Subgroup	Requirement	Comments	Meets Requirements	Describe How Requirements Met
1	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall develop, document and manage the processes and procedures for interfaces and Batch Operations Architecture.			
2	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall define job scheduling requirements, application software interdependencies, and rerun requirements for all production jobs.			
3	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall utilize and manage scheduling tools for automating job execution (e.g., job workflow processes interdependencies, rerun requirements, file exchange functions, and print management)			
4	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall maintain a master job schedule and execute all batch jobs for the DHS Enterprise Program (e.g. any jobs provided by any vendor working on/with the DHS Enterprise Platform)			
5	Application Hosting	Batch – Job Control and Scheduling	Any technology vendor, application or solution shall perform job monitoring and manage resolution of any failed jobs.			
6	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.			
7	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.			
8	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.			
9	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.			
10	Application Hosting	Disaster Recovery	Any technology vendor, application or solution shall develop action plans to address any issues arising from Disaster Recovery testing.			
11	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.			
12	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.			
13	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.			
14	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.			

15	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.		
16	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.		
17	Application Hosting	Storage Management Services	Any technology vendor, application or solution will provide data backup and restoration services in accordance with industry best practices.		
18	Application Hosting	Storage Management Services	Any technology vendor, application or solution will recommend techniques and procedures to ensure disk storage resources are utilized in an efficient and cost-effective manner.		
19	Application Hosting	Storage Management Services	Any technology vendor, application or solution shall regularly test recovery procedures and practices to demonstrate recoverability and verify that actual practices are in concert with procedures and report results, as well as meet business requirements		
20	Application Hosting	Storage Management Services	Any technology vendor, application or solution shall monitor and demonstrate compliance with Arkansas Records Retention Schedule.		
21	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		
22	Application Hosting	System Monitoring	Any technology vendor, application or solution shall monitor infrastructure for availability as well as transaction and response time performance.		
23	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)		
24	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.		

25	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.		
26	Data Governance	Master Data Management	Any technology vendor, application or solution shall provide data dictionary, data models, data flow models, process models and other related planning and design documents to DHS.		
27	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: 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		
28	General System Behavior	Audit_& Compliance	Any technology vendor, application or solution shall prevent modifications to the audit records.		
29	General System Behavior	Audit_& Compliance	Any technology vendor, application or solution must have the ability to capture electronic signatures on all documents, forms, letters, and correspondences.		
30	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		
31	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.		



32	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall develop/integrate services using standardized Web Services formats.		
33	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall provide the ability to publish services and related data to be used by different types and classes of service consumers.		
34	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall provide the capabilities for a Real-Time (or near real-time) Integrated Enterprise where common data elements about the customer's served (e.g., clients) and services rendered are easily shared across organizational units with appropriate adherence to State and Federal security and privacy restrictions.		
35	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the capability to implement synchronous and asynchronous program-to-program communication, moving messages between service oriented architecture (SOA) service consumer modules and service provider modules at runtime.		
36	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have message and data formats that will be based on logical representations of business objects rather than native application data structures.		
37	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall avoid point-to-point integrations. Application integration, both internal and external, will go through the DHS Enterprise Service Bus/Data Integration Hub.		
38	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.		
39	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.		
40	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, HTTPS 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.		
41	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution will have the capability to work with security policy manager for Web services that allows for centrally defined security policies that govern Web services operations (such as access policy, logging policy, and load balancing).		
42	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall have the capability to integrate with Master Data Management (MDM) technology for Enterprise Master Client Index (EMCI) implemented as part of the "State Hub" in a centralized or registry style implementation.		
43	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution shall be responsive and will automatically be sized for an optimum view to the display dimensions of PC, Tablet or Mobile phone.		

44	General System Behavior	Interoperability-Interfaces	Any technology vendor, application or solution components will be committed to an advanced approach to interoperability using web services and Service Oriented Architecture (SOA) aligned with DHS Enterprise Architecture Standards and industry standards and vision for interoperability.		
45	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution must be architected to support replication of the virtual machines to a secondary site.		
46	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		
47	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution shall leverage virtualization to expedite disaster recovery. Virtualization enables system owners to quickly reconfigure system platforms without having to acquire additional hardware.		
48	General System Behavior	Perf. and Avail.	Any technology vendor, application or solution will provide the ability to perform archival/incremental backups and the ability to perform open/closed database backups.		
49	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.		
50	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall allow for different roles for Users including Operators, Administrators, Managers etc.		
51	General System Behavior	Regulatory_&_Security	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: 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, MARSE 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		
52	General System Behavior	Regulatory_&_Security	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: (http://www.w3.org/TR/MCAG10/full-checklist.html)		

53	General System Behavior	Regulatory & Usability	Any technology vendor, application or solution shall adhere to the AR State accessibility standards and comply with the provisions of Arkansas Code Annotated § 25-26-201 et seq., as amended by Act 308 of 2013.		
54	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution comply with the DHS branding standards as defined by DHS.		
55	General System Behavior	Regulatory_&_Security	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		
56	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		
57	General System Behavior	Regulatory_&_Security	Any technology vendor, application or solution shall follow the DHS Enterprise Architecture Standards regarding identity, authorization and access management.		
			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.).		
58	General System Behavior	Regulatory_&_Security	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. 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.		
59	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.		
60	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.		

61	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		
62	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).		
63	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.)		
64	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		
65	General System Behavior	Solution Administration	Any technology vendor, application or solution will allow System administrators to create and manage user roles.		
66	General System Behavior	Solution Administration	Any technology vendor, application or solution communications will be protected by at least 256-bit encryption.		
67	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.		
68	General System Behavior	Regulatory_&_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.		
69	General System Behavior	User Interface	Any technology vendor, application or solution must perform address validation for demographic information (e.g., USPS, Smarty Streets, AR GIS, etc.). Suggest the validated new address and prompt user to select either user entered address or validated address, and then save accordingly.		
70	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.		
71	General System Behavior	User Interface	Any technology vendor, application or solution must have the ability to auto-save, prompt to save when leaving pages in all modules.		

72	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).		
73	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.		
74	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).		
75	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.		
76	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.		
77	Technology Platform Requirements	Data Integ, Quality, ETL	Any technology vendor, application or solution Extract Transform and Load (ETL) components will provide process flow and user interface capabilities to enable business users to perform data-quality-related tasks and fulfill stewardship functions, including: a. Packaged processes, including steps used to perform common quality tasks (providing values for incomplete data, resolving conflicts of duplicate records, specifying custom rules for merging records, profiling, auditing, for example) b. User interface in which quality processes and issues are exposed to business users, stewards and others c. Functionality to manage the data quality issue resolution process through the stewardship workflow (status tracking, escalation and monitoring of the issue resolution process) d. Ability to customize the user interface and workflow of the resolution process e. Ability to execute data quality resolution steps in the context of a process orchestrated by Business Process Management (BPM) tools (packaged integration or other ability to work with popular BPM suites, for example)		