NEW MEXICO HEALTH INSURANCE EXCHANGE (NMHIX)

REQUEST FOR PROPOSALS FOR

Independent Security Risk Assessment

RFP No. 2016-005

RFP Issued: Wednesday, February 3, 2016

Proposals Due By: Friday, February 19, 2016

Contents

1. BACKGROUND INFORMATION

1.1. Background on the New Mexico Health Insurance Exchange

The New Mexico Legislature passed SB 221 and 589 as amended, the "New Mexico Health Insurance Exchange Act," (the "Act") during the 2013 Regular Session, and Governor Susana Martinez signed the Act on March 28, 2013. The New Mexico Health Insurance Exchange (NMHIX) is created as a non-profit public corporation. In March 2015 the NMHIX board decided to discontinue pursuing their own Individual Exchange technology and continue down the path of operating as a Support State Based Marketplace (SSBM). NMHIX received acknowledgement from CMS of their updated operating model and is continuing down this path today.

Our mission is to provide qualified individuals and employers with increased access to health insurance in New Mexico. Our vision is to improve the quality of life for New Mexicans, especially when it comes to their health, their access to health care providers, and their financial security. The Exchange is governed by a 13-member board of directors that was appointed in April 2013. The Exchange's third open enrollment period began on November 1, 2015 and ends on January 31, 2016.

NMHIX has been working with GetInsured (GI) as a technology vendor. The GI HIX solution for SHOP went live on October 1, 2013. NMHIX utilizes the Federally Facilitated Marketplace (FFM) for the individual marketplace while maintaining its status as a Supported State-Based Marketplace (SSBM). In regard to internal IT infrastructure, NMHIX is contracted with ABBA Technologies, an Albuquerque-based company.

1.2. Purpose of the RFP

NMHIX is soliciting responses from qualified Offerors that are able to provide an Independent Security Risk Assessment (SRA). In order to perform security testing or analyses, the contractor and testing team members shall consist of independent third-party individual(s) responsible for developing and executing the test procedures. To be considered independent, the Contractor and testing team members shall not have any vested interest or input into the development, maintenance, or documentation of the system to be tested. Additionally, to be qualified for performing as part of security testing all testing team members must:

- Have experience in the Information Security field and experience conducting security tests and/or assessments;
- Must have knowledge of and working experience with CMS including the CMS Harmonized Information Security and Privacy Framework and Minimum Acceptable Risk Standards for Exchanges version 2.0 (MARS-E); and,
- Have a demonstrable understanding of the type of software, operating systems and infrastructure utilized by the system that is undergoing security testing to ensure that the system is adequately tested and that any security vulnerabilities identified are appropriately addressed.

2. ADMINISTRATIVE INFORMATION

2.1. Procurement Administrator

The Procurement Administrator for this project shall be:

Yolanda Miles
Sr. Director of Operations
New Mexico Health Insurance Exchange
6301 Indian School Road NE, Suite 100
Albuquerque, NM 87110
505-314-5301
RFP@nmhix.com
(Please include "SRA RFP" in the subject of any emails)

Offerors may submit questions to the Procurement Administrator at the email listed above.

2.2. Key Dates

Activity	Date
Issue RFP	February 3, 2016
Submission of Written Questions	February 10, 2016
Written Responses to Questions and Addendum to RFP Posted (as necessary)	February 12, 2016
Proposals Due	February 19, 2016 3 P.M. Mountain Time
RFP Evaluation completed	February 24, 2016
Final interviews conducted	March 3, 2016
Anticipated Contract Award	March 7, 2016
Anticipated Contract Execution Date	March 14, 2016

Contractual start dates may vary based upon negotiations between NMHIX and awarded vendor.

2.3. Contract Period and Terms & Conditions

NMHIX intends on signing a 2-month contract (March 14, 2016 – May 13, 2016) with the SRA Vendor.

2.4. Restrictions on Communications

From the issue date of this RFP until the Evaluation Committee announces its preferred Contractor, all communications related to this RFP must be with the Procurement Administrator, and all such communications must be done via email. The Procurement Administrator will respond only to written questions in emails regarding the procurement process and this RFP. Oral questions will not be accepted. Offerors may be disqualified if they contact any employee or affiliate of The Health Insurance Exchange regarding this RFP. NMHIX responses to submitted questions will be posted to the NMHIX website.

2.5. Questions and Requests for Clarifications

Offerors may submit questions to the Procurement Administrator through the email noted in

Section 2.1. The NMHIX may provide written responses to those questions, but is not obligated to do so.

2.6. Amendment and Withdrawal of this RFP

The NMHIX reserves the right to amend or withdraw the RFP at any time and for any reason. Amendments and or notices of withdrawal will be sent to the list of interested Offerors.

2.7. Amendment and Withdrawal of Proposals

Offerors may amend or withdraw their Proposals at any time before the Award Date. The amendment must be in writing, signed by Offeror, and received by the time set for the receipt of Proposals. Offerors must notify the Procurement Administrator in writing prior to the deadline for Proposals if they wish to completely withdraw their Proposals.

2.8. Submission of Proposals

The Procurement Administrator must receive all components of the Proposal by the deadline as detailed in Section 5.4. It is Offeror's responsibility to ensure that the Proposal is received prior to the deadline. Postmarking by the due date will not substitute for actual receipt of the Proposal.

2.9. Costs of Preparing the Proposal

The costs of preparation and delivery of the Proposal are solely the responsibility of the Offeror.

2.10. No Commitment to Contract

The NMHIX reserves the right to reject any or all Proposals received in response to this RFP at any time prior to the execution of the Contract. Issuance of this RFP in no way constitutes a commitment by the NMHIX to award a contract.

2.11. Rejection of Proposals

The NMHIX may reject outright and not evaluate any Proposal that does not comply with the terms of this RFP.

2.12. Nonmaterial Variances

The NMHIX reserves the right to waive or permit cure of nonmaterial variances in a Proposal if, in the judgment of the NMHIX, it is in the Exchange's best interest to do so. The determination of materiality is in the sole discretion of NMHIX.

2.13. Subcontractors

Contractor is solely responsible for fulfillment of the Contract. The NMHIX will make payments only to the Contractor. The Contractor will not subcontract any portion of the services to be performed under the Contract without the prior expressed written approval of the NMHIX. Contractor will include all proposed subcontractors in its Proposal. Subcontractors must be clearly identified within the proposal. In the event the NMHIX approves any subcontractor, Contractor will remain fully responsible for complying with the duties and obligations under the Contract.

Any use of subcontractors by Contractor will not obligate the NMHIX as a party to the subcontract, nor create any right, claim, or interest for the subcontractor against the NMHIX, its agents, employees, representatives, or successors. The parties agree that there are no third party beneficiaries, intended or otherwise, to the Contract.

2.14. Reference Checks

The NMHIX may contact any reference to assist in the evaluation of the Proposal, to verify information contained in the Proposal, or to discuss Offeror's qualifications and the qualifications of any subcontractor identified in the Proposal.

2.15. Information from Other Sources

The NMHIX reserves the right to obtain and consider information from other sources concerning an Offeror, such as Offeror's capability and performance under other contracts, the qualifications of any subcontractor identified in the Proposal, Offeror's financial stability, past or pending litigation, and other publicly available information.

2.16. Proposal Clarification Process

The NMHIX reserves the right to contact an Offeror after the submission of Proposals for the purpose of clarifying a Proposal. This contact may include written questions, interviews, site visits, or requests for corrective pages in Offeror's Proposal. The NMHIX will not consider information received from or through Offeror if the information materially alters the content of the Proposal or the type of services Offeror is offering to the NMHIX. An individual authorized to legally bind Offeror shall sign responses to any request for clarification. Failure to comply with requests for additional information may result in rejection of the Proposal.

2.17. Disposition of Proposals

All Proposals become the property of NMHIX and shall not be returned to the Offeror.

2.18. Requests for Confidential Treatment

Any Proposal submitted which contains information for which Offeror is requesting confidential

treatment must be conspicuously marked by Offeror on the outside as containing confidential information, and each page upon which confidential information appears must be conspicuously marked as containing confidential information.

Failure to properly identify specific information as confidential shall relieve the NMHIX from any responsibility to treat such information as confidential. Information not marked confidential may be viewed by the public.

As between the NMHIX and the Offeror, the NMHIX will own all right, title and interest in and to and all ideas presented in any Proposal, and shall therefore have the right to use any such ideas.

2.19. Release of Claims

By submitting a Proposal, Offeror agrees that it waives and releases all claims or causes of action against the NMHIX based on any misunderstanding concerning the information provided in this RFP or concerning the NMHIX's failure, negligent or otherwise, to provide Offeror with pertinent information in this RFP.

2.20. Offeror Presentations

At the sole discretion of the NMHIX and/or its Evaluation Committee, some Offerors may be asked to participate in oral interviews, presentations, and/or demonstrations prior to the selection of a Contractor. This process is intended to allow Offerors to demonstrate their proposed solutions and clarify any elements of their Proposal. Any cost associated with interviews, presentations, and/or demonstrations will be borne solely and entirely by Offeror. The presentation may occur at the NMHIX's offices, via the Internet, or at another location as specified by the NMHIX.

2.21. Award Notice and Acceptance Period

A "Notice of Intent to Award" will be sent to the successful Offeror. Negotiation and execution of the Contract shall be completed no later than 14 days from the date of the Notice of Intent to Award or such other time as designated by the NMHIX. If the successful Offeror fails to negotiate and execute in good faith a final agreement by that date, the NMHIX, in its sole discretion, may cancel the award and award the Contract to another Offeror the NMHIX believes meets this RFP's requirements and will provide the best value to NMHIX. A "Notice of Intent to Award" will be sent to the unsuccessful Offerors once a contract is executed or at such other time as designated by the NMHIX.

2.22. No Contract Rights until Execution

No Offeror shall acquire any legal or equitable rights regarding the Contract unless and until the Contract has been fully executed by the successful Offeror and the NMHIX.

2.23. Choice of Law and Forum

This RFP and the Contract shall be governed by the laws of the United States and of the State of New Mexico, without regard to principles of conflicts of law. Any and all litigation or actions commenced in connection with this RFP shall be brought to the appropriate federal or state courts in the State of New Mexico.

2.24. Protests

Any actual or prospective Offeror who believes it is aggrieved in connection with the solicitation or award of a Contract hereunder may protest to the Executive Director of the NMHIX. Such a protest shall be submitted in writing within five working days after the aggrieved Offeror knows or should have known of the facts giving rise thereto; provided that a protest of an award or proposed award shall in any event be submitted in writing within five working days after the award of the Contract; provided further that no protest based upon the content of the RFP or other solicitation documents shall be considered unless it is submitted in writing prior to the date set for the receipt of offers.

The Executive Director of the NMHIX or a designee may settle and resolve a protest concerning the solicitation or award of a contract hereunder. If the protest is not resolved by mutual agreement, the Executive Director of the NMHIX or a designee shall promptly issue a decision in writing to uphold or deny the protest.

2.25. Eligible Applicants

- Applications must be from an organization legally authorized to conduct business in the state of New Mexico.
- Applications from individuals will not be accepted.
- Health insurance issuers and producers are not eligible to submit a proposal. NMSA 1978, § 59A-23F-4(F).

2.26. Contract Terms and Conditions

The contract between NMHIX and a contractor will follow the format specified by the NMHIX and contain the terms and conditions set forth in Exhibit 1. The NMHIX reserves the right to negotiate with any Offeror provisions in addition to those contained in the sample contract. The contents of this RFP, as revised and/or supplemented, and the successful Offeror's proposal will be incorporated into and become part of any resultant contract.

The NMHIX discourages exceptions to contract terms and conditions. Exceptions may cause a proposal to be rejected as nonresponsive when, in the sole judgment of the NMHIX (and the

evaluation committee), the proposal appears to be conditioned on the exception, or correction of what is deemed to be a deficiency, or an unacceptable exception which would require a substantial proposal rewrite to correct is proposed.

Should an Offeror object to any of the terms and conditions in the sample contract strongly enough to propose alternate terms and conditions in spite of the above, the Offeror must propose specific alternative language. The NMHIX may or may not accept the alternative language. General references to the Offeror's terms and conditions or attempts at complete substitutions are not acceptable to the NMHIX and will result in disqualification of the Offeror's proposal.

Offerors must provide a brief discussion of the purpose and impact, if any, of each proposed change followed by the specific proposed alternate wording.

2.27. Disclosure Regarding Responsibility

Prospective Offerors shall disclose whether the Offeror, or any principal of the Offeror:

1. Is presently debarred, suspended, proposed for debarment, or declared ineligible for award of contract by any federal entity, state agency or local public body.
2. Have within a three-year period preceding this offer, been convicted of or had civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, state or local) contract or subcontract; violation of Federal or state antitrust statutes related to the submission of offers; or commission in any federal or state jurisdiction of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violation of Federal criminal tax law, or receiving stolen property.
3. Are presently indicted for, or otherwise criminally or civilly charged by any (federal state or local) government entity with, commission of any of the offenses enumerated in paragraph 2 of this disclosure.
4. Have preceding this offer, been notified of any delinquent Federal or state taxes in an amount that exceeds three thousand dollars ($3,000.00) of which the liability remains unsatisfied.
    a. Taxes are considered delinquent if both of the following criteria apply:
        i. The tax liability is finally determined. The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge of the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.
        ii. The taxpayer is delinquent in making payment. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.
5. Have within a three year period preceding this offer, had one or more contracts terminated for default by any federal or state agency or local public body.
6. Principal, for the purpose of this disclosure, means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business

entity or related entities.

7. The Offeror shall provide immediate written notice to the NMHIX if, at any time prior to contract award, the Offeror learns that its disclosure was erroneous when submitting or became erroneous by reason of changed circumstances.
8. A disclosure that any of the items in this requirement exist will not necessarily result in withholding an award under this solicitation. However, the disclosure will be considered in the determination of the Offeror's responsibility. Failure of the Offeror to furnish a disclosure or provide additional information as requested will render the Offeror nonresponsive.
9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the disclosure required by this document. The knowledge and information of an Offeror is not required to exceed that which is the normally possessed by a prudent person in the ordinary course of business dealings.
10. The disclosure requirement provided is a material representation of fact upon which reliance was placed when making an award and is a continuing material representation of the facts. If during the performance of the contract, the contractor is indicted for or otherwise criminally or civilly charged by any government entity (federal, state or local) with commission of any offenses named in this document the contractor must provide immediate written notice to the Procurement Manager or Buyer. If it is later determined that the Offeror knowingly rendered an erroneous disclosure, in addition to other remedies available to the NMHIX, the NMHIX may terminate the involved contract for cause. Still further the NMHIX may suspend or debar the contractor from eligibility for future solicitations until such time as the matter is resolved to the satisfaction of the NMHIX.

2.28. Conflict of Interest; Governmental Conduct Act

The Offeror warrants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance or services required under the Agreement. The Offeror certifies requirements of the Governmental Conduct Act, Sections 10-16-1 through 10-16-18, NMSA 1978, regarding contracting with a public officer or state employee or former state employee have been followed.

3. SCOPE OF WORK

3.1. Overview

NMHIX is soliciting responses from qualified Offerors that are able to provide an Independent Security Risk Assessment (SRA). In order to perform security testing or analyses, the contractor and testing team members shall consist of independent third-party individual(s) responsible for developing and executing the test procedures. To be considered independent, the Contractor and testing team members shall not have any vested interest or input into the development, maintenance, or documentation of the system to be tested. Additionally, to be qualified for performing as part of security testing all testing team members must:

- Have experience in the Information Security field and experience conducting security tests and/or assessments;
- Must have knowledge of and working experience with CMS including the CMS Harmonized Information Security and Privacy Framework and Minimum Acceptable Risk Standards for Exchanges version 2.0 (MARS-E); and,
- Have a demonstrable understanding of the type of software, operating systems and infrastructure utilized by the system that is undergoing security testing to ensure that the system is adequately tested and that any security vulnerabilities identified are appropriately addressed.

The Contractor shall perform a security risk assessment of applications and/or infrastructures located at the NMHIX Data Center. The Contractor shall review available application documentation, including but not limited to requirements documentation, Risk Assessments (RAs), System Security Plans (SSPs), and/or System Design Documents (SDDs) and all other documentation. The Contractor shall be familiar with MARS-E 2.0 and other Federal security policies, procedures, standards and laws pertaining to this activity.

The Evaluators and/or testing team shall review all provided documentation 5 days prior to onsite testing. NMHIX expects that the evaluators to be knowledgeable of the system(s) in scope for the SRA engagement and prepared for any/all meetings/interviews.

The Contractor shall complete the work necessary in accordance with all relevant NMHIX policies and prepare a comprehensive security test report for each system tested.

The Contractor shall provide on-going post-test support to clarify findings, make recommendations, review Corrective Action Plans (CAPs), and validate the corrective action as necessary.

3.2. Workstream for this Procurement

The Contractor's scope of work will include:

1. **Security Testing**
    - The Contractor shall complete all work necessary to perform a "Comprehensive

Scope" SRA as directed by NMHIX.

For a "Comprehensive Scope" SRA, all of the security controls within the NIST SP 800-53 rev 4 as well as the following for testing:

- The *CMS Acceptable Risk Safeguards (ARS)* security control families will be used for:
- Application testing
- Access Controls (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Security Assessment and Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- System Maintenance (MR)
- Media Protection (MP)
- Physical and Environmental Protections (PE)
- Security Planning (PL)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communication Protection (SC)
- System and Information Integrity (SI)
- Program Management (PM)

2. **Reporting**

- The Contractor shall follow all the reporting standards in accordance with the *CMS Information Security Assessment Procedure*, the *CMS Reporting Procedure for Information Security Assessments*, and the *CMS Plan of Action and Milestone (POA&M) Guidelines*.
- When the test is complete, the Contractor shall have up to five (5) working days to deliver a draft SRA report utilizing the *CMS Reporting Procedure for Information Security Assessments.* The NMHIX Business Owner shall have up to five (5) working days to review the report. After the review period, the Contractor shall meet with NMHIX Business Owner to go over the Draft SRA Report. During the Draft SRA Report meeting each finding at issue shall be discussed, issues clarified, and questions answered. NMHIX then shall have up to five (5) working days to provide any additional documentation or other mitigating evidence (i.e. screenshots) for Contractor review to address any finding. The Contractor shall then have up to five (5) working days to analyze the additional documentation, provide a response to NMHIX as to whether the documentation addressed the finding, adjust the Draft SRA Report according to the additional documentation or mitigating evidence, and deliver the Final Test (SRA) Report to the NMHIX Contract Lead(s) for acceptance. This acceptance shall be

contingent upon the report being proof read by a Technical Writer (represented by an appropriate entry in the Revision History of the document) and inclusive of all comments, as requested. After the Final Test Report is accepted, the contractor shall deliver the Final Test Package within five (5) working days. The contractor shall deliver the Final Book Package within five (5) working days after NMHIX has accepted the Final Test Package.

- The Contractor shall provide four (4) copies of the Final Test (SRA) Package on CD as well as in a 3-ring binder notebook in the NMHIX standard detail and summary format. In addition, the Contractor shall provide EXCEL spreadsheets (POA&M Weakness, a higher-level report, and Findings/Weakness, a more detailed report. The CD(s), the notebook(s) and all notebook materials are to be clearly marked as "NMHIX SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING".

3.3. Offeror Organization and Staffing

The following section provides a description of the work, deliverables, Contractor and NMHIX responsibilities required to plan and executive the activities described in this RFP as they relate to organization and staffing. During the proposal process, the Offeror shall outline their approach to completing the tasks as outlined in this section and shall include resumes and references for all key personnel identified below.

The Contractor will be required to assign key personnel to the NMHIX project. Key personnel are not required to be located in Albuquerque, New Mexico, but must be available to be onsite, at the request of NMHIX. Key personnel may be requested to be on site or with NMHIX (which may take place in Albuquerque or another location inside or outside of New Mexico. Key personnel must be available to the project as required by NMHIX.

The Contractor shall submit a staffing plan to NMHIX for review and approval. The staffing plan shall include how the Offeror plans to address staffing requirements, project roles, project responsibilities, resource allocation, staff reporting/organizational structure, and how changes in staff will be handed throughout all phases of the project, including for subcontractors (if applicable). The staffing plan shall also describe how it will train, educate and supervise staff in preparation for project work execution. In the event that the Contractor proposes to make changes to the key personnel assigned to the project at any time, the proposed change is subject to NMHIX review and approval. NMHIX also reserves to reject proposed changes in the best interest of NMHIX or the State of New Mexico.

The Offeror shall deliver in its proposal an initial Staffing Plan. The Staffing Plan must include an organization chart showing how the Offeror proposes to staff the project. The Staffing Plan must name key Offeror staff and for each staff member provide a resume, current job title, and a description of the staff member's anticipated role in this project, and estimated time dedicated to this project. If the staff member is provided by a sub-contractor, the Offeror shall also note the

staff member's organization in the Staffing Plan. The Offeror shall deliver a final Staffing Plan within five (5) calendar days from contract award. Review and updates to this plan are expected periodically, at the request of NMHIX.

Ideal key staff candidates shall have the qualifications and experience commensurate with performing an SRA assessment with the scope and complexity of the NMHIX program. NMHIX requires that at least one individual in the team have a level of security certification (e.g., CISSP, CISA or SANS GSNA). NMHIX strongly suggests Certifications for all other personnel performing tasks on this task order. The contractor can recommend personnel who do not meet the stated requirements.

Minimally, the Staffing plan must include the following positions:

- **SRA Project Manager** – The Offeror shall include the name and resume of a qualified PMP-certified project manager who will be the principal contact with the State for the SRA project. This individual should have at least five (5) years of experience performing SRA or equivalent work on IT development projects with similar size and complexity.
- **Other Key Staff** – The Offeror shall include names, resumes, and labor cost in a consistent format; shall assure that key staff meet the qualification requirements for duties and assigned; and shall assure that key staff proposed shall be devoted to the contract as proposed.

3.4. Project Management

The following section provides a description of the work, deliverables, and Offeror and NMHIX responsibilities required to plan and execute the activities described in this RFP as they relate to Project Management and Control.

Project Management is the application of knowledge, skills, tools, and techniques to project activities to meet project requirements. The Project Management tasks consist of the Offeror's approach to planning, reporting, and meeting resource requirements throughout the term of the contract. During the proposal process, NMHIX expects the Offeror to present a clear understanding of the methods and tools used to ensure that its resources are managed to complete required tasks and deliverables as outlined in this section. During the proposal process, the Offeror shall outline their approach to completing the tasks as outlined in this section.

Project Management Description

The Offeror shall be responsible for managing all aspects of the Offeror activities identified in this

RFP. Project Management activities consist of the Offeror's approach to initiating, planning, monitoring and controlling, reporting, and meeting resource requirements throughout the life of the contract. The Offeror is expected to present a clear understanding of the methods and tools used to ensure that resources are managed and that the required tasks and deliverables are completed. The Offeror will be required to utilize a formalized approach to project management, which, at a minimum, is compliant with the most recent version (5th edition) of the Project Management Institute (PMI) Project Management Book of Knowledge (PMBOK).

Project Management includes performing the tasks associated with:

- Project Initiation – Perform the initial tasks associated with determining the nature and scope of the project and identifying key stakeholders
- Project Planning – Plan time, cost, quality, resources, risks, and communications adequately to estimate the work needed to effectively execute project work
- Project Execution – Execute project work according to the final Statement of Work
- Project Monitoring and Controlling – Monitor and control all areas of the project defined in this RFP. This includes monitoring and controlling processes to ensure that potential problems can be identified in a timely manner and corrective action can be taken
- Project Closing – Ensure the orderly closeout of the contract

At a minimum, specific Project Management tasks shall include:

Preliminary Planning

The Offeror shall perform preliminary planning tasks to ensure that NMHIX and HIX Vendors are prepared to fully initiate project activities on the Contract start date without delays. Activities for this stage include outlining and initiating project communications, introducing respective project teams, detailing specific items negotiated in the contracted scope of work, and preparing all teams for full project initiation on the contract start date.

Project Kick-Off

The Offeror shall plan and hold Project Kick-Off activities, which will focus on setting the foundation for project management throughout the life of the contract. The Contractor shall assemble all project staff, NMHIX staff, relevant NMHIX vendors, and key NMHIX stakeholders, as directed, in order to review the project plan, schedule, project roles and responsibilities for both Offeror and NMHIX staff and provide an overview of initial project risks.

The project kick-off meeting shall occur within ten (10) business days of contract execution, the Contractor shall provide a memorandum documenting meeting minutes, decisions, and outcomes.

Project Deliverable Management

The Offeror is responsible for developing all project deliverables as outlined in this RFP. The Offeror shall include the following sections with each deliverable to ensure transparency and traceability:

- Revision History – Identifies the version of the draft, the date the draft was submitted, deliverable point of contact/person making change, and a description of changes made
- Table of Contents – Provides an overview of all the contents within the deliverable along with page references
- Referenced Documents – Provides a summary of the relationship of this deliverable to other relevant documents, including the document name, number, and issuance date
- Decision Log – Provides a summary of decisions point and owners for incorporation into the Project Management Decision Log
- Assumptions/Constraints/Risks – Describes any assumptions, constraints, and risks regarding the project that impact the deliverable for incorporation into the Project Management Risks and Issues Log
- Acronyms – Provides a list of all acronyms identified in the deliverable, along with the literal translation and definition

The Offeror shall also develop and submit Deliverable Expectation Documents (DEDs) for all unique deliverables for NMHIX approval prior to deliverable preparation (e.g. only one DED needs to be submitted for the monthly status report, subsequent reports are assumed to follow the same DED). The DED shall specify the content description, proposed format, proposed media and number of copies for each deliverable. For those deliverables that are not documents, the DED shall include the proposed format and delivery method.

Status Meetings

The Offeror shall attend status meetings or conference calls on a monthly basis, or more or less frequently, if necessary. Status meetings will provide updates on project progress as outlined in the monthly status reports. Specifically, monthly status reports shall include:

- Summary of work completed during the previous status reporting period and any results achieved (by relevant WBS elements);
- Updated (if necessary) project schedule;
- Summary of project budget status (actuals to projected), including project costs, hours and estimates;
- Summary of the proposed tasks and deliverables to be performed during the upcoming status reporting period;
- Analysis of critical issues, including any schedule slippage;

- Dashboard summary that tabulates data for performance and work remaining on the project, broken down by relevant WBS elements; and,
- NMHIX Board reporting, as requested by NMHIX CEO or designated agent.

The status meetings shall take place with the NMHIX S~~enio~~r. Director of Operations.

3.5. Security Standards

All analyses will be according to the security control categories as defined in the following CMS policies, procedures, and standards:

- CMS Policy for the Information Security Program (PISP),
- CMS Information Security (IS) Acceptable Risk Safeguards (ARS), CMS Minimum Security Requirement (CMSR),
- Business Partner System Security Manual (BPSSM),
- CMS Information Security Assessment Procedure,
- The current SCA Testing at the MHBE Data Center Infrastructure document,
- CMS Technical Reference Architecture (TRA),
- CMS Minimum Configuration Standards for OS (CMCSOS) and the
- CMS Reporting Procedure for Information Security Assessments.

Contractor should also utilize the Security Risk Assessment Tool provided by the Office of National Coordinator for Health Information Technology (ONC). The link to the tool is located below.

https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

3.6. SRA Project Tasks

The following section contains lists of individual SRA tasks. All listed tasks are mandatory and considered part of this solicitation.

SRA Project Management		
TASK ITEM	**#**	**TASK DESCRIPTION**
DED Develop-ment	PM-1	In anticipation of unique deliverables, SRA vendor must create a Deliverable Expectation Document (DED) that must be completed and approved by NMHIX before the formal Deliverable (DEL) is submitted.

Project Management Plan	PM-2	Develop a Project Management Plan that describes the activities, personnel, schedule, standards, and methodology for conducting the PRS reviews.
Work Plan Creation	PM-3	Develop a Work Plan which outlines particular activities and key milestones that will be met by the Contractor on specified dates.
Organi-zation Chart	PM-4	An organization chart should be created that outlines personnel and their accompanying role.
Repository Manage-ment	PM-5	Place relevant completed deliverables including any status reports on NMHIX ShareFile site.
Issue & Risk Manage-ment	PM-6	Prepare and deliver an independent issue and risk log to NMHIX S~~enio~~r. Director of Operations.
	PM-7	Update and report risks and issues throughout entirety of project.
Change Manage-ment	PM-8	The Contractor must create and update a log that records deviations from the specified Project Scope, Work Plan, Audit Approach, or other deliverables. This log is to be delivered to the NMHIX S~~enio~~r. Director of Operations.

SRA Assessment		
TASK ITEM	**TASK #**	**TASK DESCRIPTION**
Security Testing	SE-1	Draft a test plan describing the approach to security testing
	SE-2	Deliver a final test plan
	SE-3	Execute testing of controls according to CMS MAR-E 2.0 framework
Security Reporting	SE-4	Draft a Test Report during preliminary stages of testing
	SE-5	Deliver a Final Test Report describing the execution of testing with preliminary results
	SE-6	Deliver a Final Test Package that includes Corrective Action Plan (CAP) management worksheets for each system tested
	SE-7	Deliver a Final Report Package summarizing the findings and including the details from all previous activities

3.7. SRA Project Deliverables

The following table identifies the anticipated work products that the successful Security Contractor will produce under the resultant Security contract. All the task activities listed in Section 2.6 should be addressed comprehensively within these work products. NMHIX reserves the right to request additional analyses, as needed. Likewise, the SRA Offeror may propose the development of additional work products in specific areas. NMHIX must authorize in advance the development of any additional work products.

Where applicable, the deliverable must be developed in accordance with standards utilized by the HIX IT. When no applicable standard exists, the methodology and processes used in the analysis and creation of the deliverable must be delivered to the Exchange prior to its use, and described in the final deliverable. All work products, standards, processes, plans, and applicable reference materials will be made available upon request of the Exchange.

Copies of all work products will be delivered to NMHIX. Frequencies of work products are provided in the table below, and must be followed unless otherwise changed by NMHIX. NMHIX reserves the right to modify schedules as seen fit. The Exchange reserves the right to extend the due date if appropriate, due to document size, schedule or changes in scope. The SRA Contractor must notify the Exchange of an anticipated delay of a deliverable, within one business day of identifying a delay.

Deliverables	Quantity
Project Kick-Off	1
Project Management Plan	1
Work Plan	1
Issue & Risk Log	1
Change Log	1
Draft Test Plan	1
Final Test Plan	1
Draft Test Report	1
Final Test Report	1
Final Test Package with CAP Management Worksheet	1
Final Report Package	1
Archive Documents	1

Below is an estimate of the project's timeline. Estimated deliverable due dates are noted. This is subject to change, but should be used for scheduling and pricing purposes.

Deliverables	March	April/May
Project Kick-Off	X	
Project Management Plan	X	X
Work Plan	X	X
Issue & Risk Log	X	X
Change Log	X	X
Draft Test Plan	X	
Final Test Plan	X	
Draft Test Report		X
Final Test Report		X
Final Test Package with CAP Management Worksheet		X
Final Report Package		X
Archive Documents		X

For each validation area described in section 2.6, the SRA Offeror should include in its Final Report the current state of NMHIX's effort, including any pertinent historical background information.

Responses should be quantified whenever possible. The final report should also contain detailed recommendations in each area specifying what can be done immediately and in the long term to improve NMHIX's operation. The report should also include a table of risks, recommend responses, and estimated time frames for implementing responses. Any technologies, methodologies, or resources recommended should reflect industry standards and be appropriate for the unique circumstances and constraints of the HIX Project. The recommendations should also specify a method of measuring NMHIX's progress against the recommendations.

3.8. Minimum Standard to SRA Report Requirements

Final written deliverables shall not contain structural errors such as poor grammar, misspellings, or incorrect punctuation, and must:

A. Be presented in a format appropriate for the subject matter and depth of discussion;
B. Be organized in a manner that presents a logical flow of the deliverable's content; and,
C. Be based upon relevant, factual information that is current and accurate at the time of submittal.

4. GENERAL CONTRACTUAL INFORMATION

4.1. NMHIX's Responsibilities

1. NMHIX shall make all files and records accessible to the Contractor, on site.
2. NMHIX shall provide assistance to the Contractor, namely, gathering supporting documentation from the files and preparing schedules.
3. NMHIX shall make appropriate personnel available for interviews and information-gathering purposes.

4.2. The Contractor's Responsibilities

1. Perform all duties included in this RFP.

4.3. Payment for Services

Payment Procedures

Payment is predicated upon completion of the described work and delivery of the required documentation.

Invoices must be signed, by an individual authorized to legally bind the Contractor, and submitted to the NMHIX CFO with adequate supporting documentation, including but not limited to the following:

a. The Contractor's invoice number
b. NMHIX's personal service contract number
c. "Remit to" address
d. Description of the services performed
e. Deliverables submitted and approved

Method of Payment

After appropriate review and approval of the invoice, NMHIX shall process such invoices for payment. Every reasonable effort shall be made to provide payment to the Contractor within 30 days after receipt and approval of a properly supported invoice.

The chosen Contractor may invoice the NMHIX monthly for all deliverables submitted and approved by the NMHIX in the prior month.

4.4. Modifications to Statement of Work

Any modifications to the statement of work shall be thoroughly discussed with the selected Contractor and agreed to in contract form by the Offeror and NMHIX prior to implementation. If necessary, the contract amount shall be amended to reflect such modification.

5. TECHNICAL PROPOSAL

5.1. Responsiveness

In order to be considered, the proposal submitted by an Offeror must be completely responsive to this RFP. All conditions printed on the RFP are hereby made a part of the conditions under which the proposal is submitted and shall be incorporated, in whole or in part at NMHIX's discretion, into any contract on this project. Further, the contents of a proposal, in whole or in part at NMHIX's discretion, shall become part of any contract resulting from that proposal. Failure of an Offeror to accept these obligations may result in disqualification from the procurement process.

5.2. Format of the Technical Proposal

The technical proposal shall respond completely to the requirements stated in this section. In order to permit effective comparisons of competing proposals, the following format shall be adhered to:

Section Number	Section Title
1	Title Page – Include name of the Offeror, local address, telephone number, fax number, email address (if any), name of contact person, and date.
2	Table of Contents – Clearly identify the material by section and page number
3	Transmittal Letter—In the form of a standard business letter and shall be signed by an individual authorized to legally bind the Offeror. It shall include the following: a) A statement indicating the Offeror is a corporation or other legal entity. b) A statement that no attempt has been made or shall be made by the Offeror to induce any other person or an Offeror to submit or not to submit a proposal. c) A statement of affirmative action that the Offeror does not discriminate in its employment practices because of race, color, religion, age (except as provided by law), sex, marital status, political affiliation, national origin, or persons with disabilities. In addition, the Offeror shall provide a statement of compliance with the requirements of Title VI of the Civil Rights Act of 1964.

	d) In accordance with paragraph 2.27 and 2.28 of this RFP, a statement disclosing any information relevant to paragraph 2.27 or a statement that the Offeror has no such information to disclose and confirmation of compliance with 2.28.
4	The Offeror's Background and Experience: The details of the Offeror's background and experience shall cover the following: a) Date the Offeror was established. b) Location of the Offeror's clientele (local, regional, national, or international). c) Total number of professional staff. d) Provide a listing and description of all firm-wide experience during the last three consecutive calendar years in working on similar types of SRA projects: e) Provide a minimum of three references for SRA projects included above. The reference should include the individuals name, title, organization, email address, and telephone number.
5	Individual Staff Qualifications a) Provide a brief biographical sketch describing the qualifications of each project member. Include the auditor's current office location – preference may be given to Albuquerque-based staff. b) Include a proposal organizational chart.
6	Work Plan and Approach a) Provide the proposed work plan including phases and detailed steps needed to complete all activities requested in this RFP. Include estimated effort (in hours) needed to complete each task. b) Provide a narrative explanation of the approach to this engagement, including approaches to effectively working with the NMHIX and GetInsured (HIX IT vendor) and ABBA Technologies (internal IT infrastructure vendor). c) Provide at least one example of a template to be used as the SRA Report.
7	Cost Proposal Include the table shown in Section 6.1 and a brief narrative explanation for how the Offeror arrived at the budget.

5.3. Deviation from Specifications

If the technical proposal deviates from the detailed specifications and requirements of this RFP, the transmittal letter shall identify and explain these deviations. NMHIX reserves the right to reject any proposal containing such deviations or to require modifications before acceptance.

5.4. Proposal Submission

To be considered for contract award, five (5) copies of the technical proposal (which includes the Cost Proposal) must be at the office of NMHIX offices at 6301 Indian School Road NE, Suite 100, Albuquerque, NM 87110, addressed to the Procurement Administrator by 3 p.m. MST on February 19, 2016. Offeror must include a flash drive with a digital copy of the proposal. Proposals submitted via email, fax, or any other form of communication will be rejected.

6. COST PROPOSAL

6.1. Cost Proposal

The NMHIX will measure and pay for these SRA services based on the deliverables outlined in this RFP. The NMHIX requests that Offerors provide costs according to the template provided below.

	Deliverable	Quantity (# Units)	Cost Per "Unit"	Total Cost	Estimated Effort (in Hours)*
1	Project Kick-Off	1		$ -	
2	Project Management Plan	1		$ -	
3	Work Plan	1		$ -	
4	Issue & Risk Log	1		$ -	
5	Change Log			$ -	
6	Draft Test Plan	1		$ -	
7	Final Test Plan	1		$ -	
8	Draft Test Report	1		$ -	
9	Final Test Report	1		$ -	
10	Final Test Package with CAP Management Worksheet	1		$ -	
11	Final Report Package	1		$ -	
12	Archive Documents	1		$ -	
				$ -	

*** Estimated hours to provide NMHIX with an idea of resources and efforts. Not to be used in pricing.**
****Initial contract may not include this deliverable.**

Ad hoc services

Provide an all-inclusive hourly rate for ad hoc SRA services

All proposed costs shall be inclusive of all Offeror costs, including staffing, fringe and other overhead, travel, and other expenses.

6.2. Deviation from Specifications

If the cost proposal deviates from the specifications and requirements of this RFP, the transmittal letter shall identify and explain these deviations. NMHIX reserves the right to reject any proposal containing such deviations or to require modifications before acceptance.

6.3. Submission of Cost Proposal

The Cost Proposal should be submitted as part of the Technical Proposal, as shown in Section 5.4.

7. EVALUATION

7.1. Overall Evaluation Criteria

The proposals shall be evaluated by a RFP committee, appointed by the Procurement Administrator.

7.2. Evaluation of the Technical Proposal

Each technical proposal will be evaluated in the following categories. The maximum number of points available in each category is shown beside that category below:

Offeror's Background and Experience	50 points
Work Plan and Testing Approach	30 points
Cost	20 points
TOTAL	**100 points**

The Procurement Administrator will determine the method for proposal evaluation to be followed by the Evaluation Committee. The Evaluation Committee will make a recommendation to the Operations Committee. Once approved by the Operations Committee of the Board of Directors, the Offeror will be notified of the Intent to Award the contract to that Offeror.

EXHIBIT 1

Sample Agreement

AGREEMENT BETWEEN
THE
NEW MEXICO HEALTH INSURANCE EXCHANGE
AND
_____.

THIS AGREEMENT, referred to hereinafter as "Agreement," is made and entered into by and between the **New Mexico Health Insurance Exchange**, hereinafter referred to as "NMHIX," and _____, hereinafter referred to as the "Contractor," and is effective as of the date when it is executed by NMHIX. This Agreement is the result of NMHIX Procurement # _____.

IT IS AGREED BETWEEN THE PARTIES:

1. Scope of Work

A. The Contractor shall perform all services detailed in Exhibit A, Scope of Work, and shall comply with the terms and conditions detailed in Exhibit B, Privacy and Security Standards, both of which are attached to this Agreement and incorporated herein by reference.

B. In addition to any other reporting provisions required by this Agreement or by law, Contractor shall report to the NMHIX monthly, or according to a different schedule as established by the NMHIX, regarding Contractor's performance and fulfillment of its obligations under this Agreement.

2. Deliverables and Consideration

A. NMHIX shall pay to the Contractor in full payment for services satisfactorily performed and for allowable expenses, costs, and other fees an amount not to exceed $_____. Expenses, costs, and other fees must be approved by NMHIX and shall be in compliance with federal regulations regarding expenditure of federal grant funds. This amount is a maximum and not a guarantee that the work assigned to be performed by the Contractor under this Agreement shall equal the amount stated herein. The New Mexico gross receipts tax, if applicable, levied on the amounts payable under this Agreement shall be paid by the Contractor. The parties do not intend for the Contractor to, and Contractor shall not be obligated to, continue to provide services beyond what Contractor has agreed to provide without compensation when the total compensation amount is reached. The Contractor is responsible for notifying NMHIX before the services provided under this Agreement reach the total compensation amount. In no event will the Contractor be paid in excess of the total compensation amount without this Agreement being amended in writing prior to those services in excess of the total compensation amount being provided.

B. All payments are subject to availability of funds pursuant to Paragraph 5, Funding, set forth below, and to any negotiations between the parties from year to year pursuant to Paragraph 1, Scope of Work. All invoices MUST BE received by NMHIX no later than fifteen (15) business days after each calendar month in which the services were delivered. The Contractor must submit a detailed statement accounting for all services performed.

3. Term

This Agreement shall terminate on ____ unless terminated pursuant to Paragraph 4, Termination, or Paragraph 5, funding. This Agreement may be extended for an additional term or terms by mutual agreement of the parties.

4. Termination

A. This Agreement may be terminated by the NMHIX, at its discretion and at any time for any reason, upon written notice delivered to the Contractor thirty (30) days prior to the intended date of termination. Except as otherwise allowed or provided under this Agreement, NMHIX's sole liability upon such termination shall be to pay for acceptable work performed prior to the notice of termination; provided, however, that a notice of termination shall not nullify or otherwise affect any party's obligations under this Agreement prior to termination. The Contractor shall submit an invoice for all completed work within thirty (30) days of the effective date of termination. Notwithstanding the foregoing, this Agreement may be terminated immediately upon written notice to the Contractor if the Contractor becomes unable to perform the services contracted for, as reasonably determined by NMHIX, or if, during the term of this Agreement, the Contractor or any of its officers, employees, or agents is indicted for fraud, embezzlement or other crime due to misuse of public funds.

In the event of a material default or breach of this Agreement by Contractor, NMHIX shall notify Contractor of such material default or breach and Contractor shall have a period of 30 days, or a longer period if NMHIX and Contractor agree it is necessary, to cure such material breach or default. If Contractor is unable to cure the material default or breach within 30 days or the agreed upon period, NMHIX may notify Contractor of its intent to immediately terminate this Agreement. *THIS PROVISION IS NOT EXCLUSIVE AND DOES NOT WAIVE NMHIX's OTHER LEGAL RIGHTS AND REMEDIES CAUSED BY THE CONTRACTOR'S DEFAULT/BREACH OF THIS AGREEMENT.*

B. Immediately upon receipt of notice of termination of this Agreement, the Contractor shall: 1) not perform additional services without written approval of NMHIX; 2) comply with all directives issued by NMHIX in the notice of termination as to the performance of work under this Agreement; and 3) take such action as NMHIX shall direct for the protection, preservation, retention or transfer of all property titled to NMHIX and records generated under this Agreement. Upon receipt of such notice, the parties agree to negotiate in good faith a transition plan for the wind down of the services. Any non-expendable personal property or equipment provided to or purchased by the Contractor with contract funds shall become property of NMHIX upon termination and shall be submitted to NMHIX as soon as practicable.

5. Funding

The terms of this Agreement are contingent upon (1) continued authorization of the NMHIX by the Legislature of New Mexico, (2) sufficient legislative appropriations, if any, for the NMHIX operations and activities, and (3) the ability of NMHIX to obtain funds, by federal grants or other means, necessary to carry out NMHIX operations and activities and comply with the terms and conditions of this Agreement. If sufficient appropriations and authorization are not made by the Legislature and funding is not available, this Agreement shall terminate immediately upon written notice being given by NMHIX to the Contractor. NMHIX's decision as to whether sufficient appropriations, authorization, and funding are available shall be accepted by the Contractor and shall be final.

6. Status of the Contractor

The Contractor and its agents and employees are independent contractors performing professional services for NMHIX and are not employees of NMHIX. The Contractor and its agents and employees shall

not accrue leave, retirement, insurance, bonding, use of state vehicles, or any other benefits afforded to employees of the NMHIX as a result of this Agreement. The Contractor acknowledges that all sums received hereunder are reportable by the Contractor for tax purposes, including without limitation, self-employment and business income tax. The Contractor agrees not to purport to bind NMHIX unless the Contractor has express written authority to do so, and then only within the strict limits of that authority.

7. Assignment

The Contractor shall not assign or transfer any interest in this Agreement or assign any claims for money due or to become due under this Agreement without the prior written approval from NMHIX.

8. Subcontracting

The Contractor shall not subcontract any portion of the services to be performed under this Agreement without the prior written approval of NMHIX. No such subcontract shall relieve the primary Contractor from its obligations and liabilities under this Agreement, nor shall any subcontract obligate direct payment from NMHIX.

9. Release

Final payment of the amounts due under this Agreement, or acceptance of the services to be performed under this Agreement, shall operate as a release of NMHIX, its officers, and employees from all liabilities, claims, and obligations whatsoever arising from or under this Agreement. The contractor agrees not to purport to bind NMHIX to any obligation not assumed herein by NMHIX unless the Contractor has express written authority to do so, and then only within the strict limits of that authority.

10. Confidentiality

A. Any confidential information provided by NMHIX to Contractor or developed by Contractor in the performance of this Agreement shall be kept confidential, and shall not be made available to any individual or organization by Contractor without the prior written approval of NMHIX.

B. Contractor agrees and acknowledges that during the course of performing services under this Agreement Contractor may create, collect, receive, use or otherwise gain access to personally identifiable information, federal tax information, or other private and confidential information. Contractor shall use or disclose such information only to the extent required for the performance of the services under this Agreement and then only to the extent allowed by law. Contractor further agrees that it is a condition of this Agreement that with regard to such information Contractor, and any subcontractors engaged by Contractor to perform services under this Agreement, shall comply with and impose privacy and security standards as outlined in Exhibit B and equal to or more stringent than the standards described in 45 C.F.R. 155.260(a), as those standards may be amended from time to time.

11. Product of Service -- Copyright

A. All materials developed or acquired by the Contractor specifically and solely for the benefit of NMHIX pursuant to the terms of this Agreement shall become the property of NMHIX and shall be delivered to NMHIX no later than the termination date of this Agreement.

B. This contract is in support of New Mexico's implementation of the Patient Protection and Affordable Care Act of 2010, and is subject to the certain property rights provisions of the Code of Federal Regulations and a Grant from the Department of Health and Human Services, Centers for Medicare &

Medicaid Services. This Contract is subject to, and incorporates by reference, 45 CFR 74.36 and 45 CFR 92.34 governing rights to intangible property. Intangible property includes but is not limited to: computer software; patents, inventions, formulae, processes, designs, patterns, trade secrets, or know-how; copyrights and literary, musical, or artistic compositions; trademarks, trade names, or brand names; franchises, licenses, or contracts; methods, programs, systems, procedures, campaigns, surveys, studies, forecasts, estimates, customer lists, or technical data; and other similar items. The Contractor may copyright any work that is subject to copyright and was developed, or for which ownership was purchased, under this Contract. The Contractor must deliver all intangible property, including but not limited to, intellectual property, to NMHIX in a manner that ensures the Centers for Medicare & Medicaid Services, an agency of the Department of Health and Human Services, obtains a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use the work for Federal purposes, and to authorize others to do so. Federal purposes include the purpose of administering New Mexico exchanges under the Affordable Care Act of 2010. The Contractor is further subject to applicable regulations governing patents and inventions, including those issued by the Department of Commerce at 37 CFR Part 401.

12. Conflict of Interest; Governmental Conduct Act

A. The Contractor represents that it presently has no interest and, during the term of this Agreement, shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance or services required under the Agreement.

B. The Contractor further represents that it has complied with, and, during the term of this Agreement, will continue to comply with, and that this Agreement complies with all applicable provisions of the Governmental Conduct Act, Chapter 10, and Article 16 NMSA 1978. Without in anyway limiting the generality of the foregoing, the Contractor specifically represents that:

1) in accordance with Section 10-16-4.3 NMSA 1978, the Contractor does not employ, has not employed, and will not employ during the term of this Agreement any NMHIX employee while such employee was or is employed by NMHIX and participating directly or indirectly in NMHIX's contracting process;

2) this Agreement complies with Section 10-16-7(A) NMSA 1978 because (i) the Contractor is not a public officer or employee of the State; (ii) the Contractor is not a member of the family of a public officer or employee of NMHIX; (iii) the Contractor is not a business in which a public officer or employee or the family of a public officer or employee has a substantial interest; or (iv) if the Contractor is a public officer or employee of NMHIX, or a business in which an employee of NMHIX has a substantial interest, public notice was given as required by Section 10-16-7(A) NMSA 1978 and this Agreement was awarded pursuant to a competitive process;

3) in accordance with Section 10-16-8(A) NMSA 1978, (i) the Contractor is not, and has not been represented by, a person who has been a public officer or employee of NMHIX within the preceding year and whose official act directly resulted in this Agreement.

4) this Agreement complies with Section 10-16-9(A) NMSA 1978 because (i) the Contractor is not a legislator; (ii) the Contractor is not a member of a legislator's family; (iii) the Contractor is not a business in which a legislator or a legislator's family has a substantial interest; or (iv) if the Contractor is a legislator, a member of a legislator’s family, or a business in which a legislator or a legislator's family has a substantial interest, disclosure has been made as required by Section 10-16-9(A) NMSA 1978, this Agreement is not a sole source or small purchase contract, and this Agreement was awarded in accordance with the provisions of the Procurement Code;

5) in accordance with Section 10-16-13 NMSA 1978, the Contractor has not directly participated in the preparation of specifications, qualifications or evaluation criteria for this Agreement or any procurement related to this Agreement; and

6) in accordance with NMSA 1978 Section 10-16-3 and 10-16-13.3, the Contractor has not contributed, and during the term of this Agreement shall not contribute, anything of value to a public officer or employee of the NMHIX.

C. The Contractor further represents that it has complied with, and, during the term of this Agreement, will continue to comply with all applicable federal provisions related to conflicts of interest, including but not limited to those contained in 45 C.F.R. 92.36, the Affordable Care Act, and the HHS Grants Policy Statement, published January 1, 2007.

D. The Contractor's representations in Sections A, B, and C of this Paragraph 12 are material representations of fact upon which NMHIX relied when this Agreement was entered into by the parties. The Contractor shall provide immediate written notice to NMHIX if, at any time during the term of this Agreement, the Contractor learns that the Contractor's representations in Sections A, B, or C of this Paragraph 12 were erroneous on the effective date of this Agreement or have become erroneous by reason of new or changed circumstances. If it is later determined that the Contractor's representations in Sections A, B, and C of this Paragraph 12 were erroneous on the effective date of this Agreement or have become erroneous by reason of new or changed circumstances, in addition to other remedies available to NMHIX and notwithstanding anything in the Agreement to the contrary, NMHIX may immediately terminate the Agreement.

E. The Contractor shall provide immediate written notice to NMHIX if, at any time during the term of this Agreement, the Contractor becomes aware of circumstances that suggest a potential conflict of interest or the appearance of impropriety.

13. Amendment

This Agreement shall not be altered, changed, or amended except by instrument in writing executed by the parties hereto and all other required signatories.

14. Merger

This Agreement incorporates all the agreements, covenants and understandings between the parties hereto concerning the subject matter hereof, and all such covenants, agreements and understandings have been merged into this written Agreement. No prior agreement or understanding, oral or otherwise, of the parties or their agents shall be valid or enforceable unless embodied in this Agreement.

15. Penalties for Violation of Law

The New Mexico criminal statutes impose felony penalties for illegal bribes, gratuities, and kickbacks.

16. Equal Opportunity Compliance

The Contractor agrees to abide by all applicable federal and state laws and rules and regulations pertaining to equal employment opportunity. In accordance with all such laws of the State of New Mexico and the United States, the Contractor assures that no person shall, on the grounds of race, religion, color, national origin, ancestry, sex, age, physical or mental handicap, or serious medical condition, spousal affiliation, sexual orientation or gender identity, be excluded from employment with or participation in, be

denied the benefits of, or be otherwise subjected to discrimination under any program or activity performed under this Agreement. If the Contractor is found not to be in compliance with these requirements during the life of this Agreement, the Contractor agrees to take appropriate steps to correct these deficiencies.

Contractor shall comply with Executive Order 11246, "Equal Employment Opportunity," as amended by E.O. 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and as supplemented by regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

17. Applicable Law; Dispute Resolution

A. **Applicable law.** The laws of the State of New Mexico shall govern this Agreement, without giving effect to its choice of law provisions.

B. **Dispute resolution.** Parties to this Agreement shall utilize methods of alternative dispute resolution to resolve disputes arising under this Agreement. NMHIX and Contractor agree to resolve disputes first through good faith negotiation, and if unsuccessful, through mediation and/or arbitration. No dispute arising under or relating to this Agreement may be brought in a court of law. The process for alternative dispute resolution is as follows:

1) Negotiation. The parties are encouraged to resolve disputes through negotiation prior to mediation or arbitration. In the event of any dispute, claim, question, or disagreement arising from or relating to a contract or the breach thereof, the parties shall use their best efforts to settle the dispute, claim, question, or disagreement. To this effect, NMHIX and Contractor shall consult and negotiate with each other in good faith and, recognizing their mutual interests, attempt to reach a just and equitable solution satisfactory to both parties. If they do not reach such solution within a period of 30 days, then, upon notice by either party to the other, all disputes, claims, questions, or differences shall be mediated or finally settled by arbitration administered by the American Arbitration Association (AAA) in accordance with the provisions of its Commercial Arbitration Rules.

2) Mediation. If a dispute arises out of or relates to this Agreement, or the breach thereof, and if the dispute cannot be settled through negotiation, the parties may first try in good faith to settle the dispute by mediation administered by the American Arbitration Association under its Commercial Mediation Procedures. Parties may agree upon a mediator and the terms of the mediation, or may use an AAA administrator to assist the parties regarding selection of the mediator, scheduling, pre-mediation information exchange and attendance of appropriate parties at the mediation conference. The mediation shall be scheduled within 30 days of notice to the other party that one party seeks to mediate the dispute.

3) Arbitration. If negotiation and mediation fail to resolve the dispute, or the time frames establish for negotiation or mediation pass, a controversy or claim arising out of this Agreement, or the breach of this Agreement, shall be settled by arbitration administered by the American Arbitration Association in accordance with its Commercial Arbitration Rules and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

4) Time periods. The time periods established in this Paragraph 17 may be amended by mutual agreement of the parties.

18. Workers Compensation

The Contractor agrees to comply with state laws and rules applicable to workers compensation benefits for its employees. If the Contractor fails to comply with the Workers Compensation Act and applicable rules when required to do so, this Agreement may be terminated by NMHIX.

19. Records and Financial Audit

A. The Contractor shall maintain detailed time and expenditure records, if any, that indicate the date; time, nature and cost of services rendered during the Agreement's term and effect and retain them for a period of ten (10) years from the date of completion of this Agreement. The records, if any, shall be subject to inspection by the NMHIX, the State Auditor, HHS, the OIG, the Comptroller General of the United States, and any of their duly authorized representatives. NMHIX shall have the right to audit billings both before and after payment. Payment under this Agreement, if any, shall not foreclose the right of NMHIX to recover excessive or illegal payments.

B. Contractor shall contract for any required independent audits, including but not limited to audits pursuant to OMB Circulars A-21, A-87, A-110, A-122, and A-133, if applicable. The Contractor shall ensure that the auditor is licensed to perform audits in the State of New Mexico and shall be selected by a competitive bid process. The Contractor shall enter into a written contract with the auditor specifying the scope of the audit, the auditor's responsibility, the date by which the audit is to be completed and the fee to be paid to the auditor for this service. The audit of the contract shall cover compliance with Federal Regulations and all financial transactions hereunder for the entire term of the Agreement in accordance with procedures promulgated by OMB Circulars or by Federal program officials for the conduct and report of such audits. An official copy of the independent auditor's report shall be made available to the State Auditor and upon request.

20. Indemnification

A. General Indemnification. The Contractor shall defend, indemnify and hold harmless NMHIX, its Board, employees, officers and agents from all third party actions, proceeding, claims, demands, costs, damages, attorneys' fees and all other liabilities and expenses of any kind from any source which are caused by the negligent act or negligent failure to act of the Contractor, its officers, employees, servants, subcontractors or agents, to the extent resulting in injury or damage to persons or personal property during the time when the Contractor or any officer, agent, employee, servant or subcontractor thereof has or is performing services pursuant to this Agreement. In the event that any action, suit or proceeding related to the services performed by the Contractor or any officer, agent, employee, servant or subcontractor under this Agreement is brought against the Contractor for which Contractor is obligated to indemnify NHMIX, the Contractor shall, as soon as practicable but no later than two (2) business days after it receives notice thereof, notify the legal counsel of NMHIX and the Risk Management Division of the New Mexico General Services Department by certified mail.

B. Indemnification for Professional Acts, Errors, or Omissions. Except for professional acts, errors or omissions that are the result of established gross negligence or willful or wanton conduct on the part of the Contractor or its employees, agents, representatives or subcontractors, the General Indemnification shall not apply to professional acts, errors or omission unless covered by Contractor's Professional Liability insurance.

21. Invalid Term or Condition

If any term or condition of this Agreement shall be held invalid or unenforceable, the remainder of this Agreement shall not be affected and shall be valid and enforceable.

22. Enforcement of Agreement

A party's failure to require strict performance of any provision of this Agreement shall not waive or diminish that party's right thereafter to demand strict compliance with that or any other provision. No waiver by a party of any of its rights under this Agreement shall be effective unless express and in writing, and no effective waiver by a party of any of its rights shall be effective to waive any other rights.

23. Notices

Any notice required to be given to any party by this Agreement shall be in writing and shall be delivered in person, by courier service, nationally recognized overnight express common carrier or by U.S. mail, either first class or certified, return receipt requested, postage prepaid, as follows:

To NMHIX:
Amy Dowd
CEO, NMHIX
New Mexico Health Insurance Exchange
6301 Indian School Road NE, Suite 100
Albuquerque, NM 87110

To Contractor:
[name, address, and email]

24. Authority

If the Contractor is other than a natural person, the individual(s) signing this Agreement on behalf of the Contractor represents that he or she has the power and authority to bind the Contractor, and that no further action, resolution, or approval from the Contractor is necessary to enter into a binding contract.

25. Debarment and Suspension

A. Consistent with either 7 C.F.R. Part 3017 or 45 C.F.R. Part 76, as applicable, and as a separate and independent requirement of this Agreement the Contractor certifies by signing this Agreement, that it and its principals, to the best of its knowledge and belief: (1) are not debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal department or agency; (2) have not, within a three-year period preceding the effective date of this Agreement, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, state, or local) contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property; (3) have not been indicted for, or otherwise criminally or civilly charged by a governmental entity (Federal, State or local) with, commission of any of the offenses enumerated above in this Paragraph 25(A); (4) have not, within a three-year period preceding the effective date of this Agreement, had one or more public agreements or transactions (Federal, State or local) terminated for cause or default; and (5) have not been excluded from participation from Medicare, Medicaid or other federal health care programs pursuant to Title XI of the Social Security Act, 42 U.S.C. § 1320a-7.

B. The Contractor's certification in Paragraph 25(A), above, is a material representation of fact upon which NMHIX relied when this Agreement was entered into by the parties. The Contractor's certification in Paragraph 25(A), above, shall be a continuing term or condition of this Agreement. As such at all times during the performance of this Agreement, the Contractor must be capable of making the certification

required in Paragraph 25(A), above, as if on the date of making such new certification the Contractor was then executing this Agreement for the first time. Accordingly, the following requirements shall be read so as to apply to the original certification of the Contractor in Paragraph 25(A), above, or to any new certification the Contractor is required to be capable of making as stated in the preceding sentence:

(1) The Contractor shall provide immediate written notice to NMHIX's CEO if, at any time during the term of this Agreement, the Contractor learns that its certification in Paragraph 25(A), above, was erroneous on the effective date of this Agreement or has become erroneous by reason of new or changed circumstances.

(2) If it is later determined that the Contractor's certification in Paragraph 25(A), above, was erroneous on the effective date of this Agreement or has become erroneous by reason of new or changed circumstances, in addition to other remedies available to NMHIX, NMHIX may terminate the Agreement.

C. As required by statute, regulation or requirement of this Agreement, and as contained in Paragraph 25(A), above, the Contractor shall require each proposed first-tier subcontractor whose subcontract will equal or exceed $25,000, to disclose to the Contractor, in writing, whether as of the time of award of the subcontract, the subcontractor, or its principals, is or is not debarred, suspended, or proposed for debarment by any Federal department or agency. The Contractor shall make such disclosures available to NMHIX when it requests subcontractor approval from NMHIX. If the subcontractor, or its principals, is debarred, suspended, or proposed for debarment by any Federal, state or local department or agency, NMHIX may refuse to approve the use of the subcontractor.

26. Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions

A. The applicable definitions and exceptions to prohibited conduct and disclosures contained in 31 U.S.C. § 1352 and 45 C.F.R. Part 93 or Subparts B and C of 7 C.F.R. Part 3018, as applicable, are hereby incorporated by reference in subparagraph (B) of this certification.

B. The Contractor, by executing this Agreement, certifies to the best of its knowledge and belief that:

(1) No Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment or modification of any Federal contract, grant, loan, or cooperative agreement; and

(2) If any funds other than Federal appropriated funds (including profit or fee received under a covered Federal transaction) have been paid, or will be paid, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on his or her behalf in connection with this solicitation, the Contractor shall complete and submit, with its offer, OMB standard form LLL, Disclosure of Lobbying Activities, to the Contracting Officer.

C. The Contractor shall require that the language of this certification be included in the award documents for all sub-awards allowed under this Agreement at all tiers (including subcontracts, sub-grants, and contracts under grants, loans, and cooperative agreements) and that all sub-recipients shall certify and disclose accordingly.

D. This certification is a material representation of fact upon which reliance is placed when this Agreement is made and entered into. Submission of this certification is a prerequisite for making and entering into this Agreement imposed under 31 U.S.C. § 1352. It shall be a material obligation of the Contractor to keep this certification current as to any and all individuals or activities of the Contractor providing services under this Agreement during the pendency of this Agreement. Any person who makes an expenditure prohibited under this provision or who fails to file or amend the disclosure form to be filed or amended by this provision, shall be subject to: (1) a civil penalty of not less than $10,000 and not more than $100,000 for such failure; and/or (2) at the discretion of NMHIX, termination of the Agreement.

27. Non–Discrimination

A. The Contractor agrees to comply fully with Title VI of the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973, Public Law 93-112, as amended; and the Americans With Disabilities Act of 1990, Public Law 101-336; in that there shall be no discrimination against any employee who is employed in the performance of this Agreement, or against any applicant for such employment, because of age, color, national origin, ancestry, race, religion, creed, disability, sex, or marital status.

B. This provision shall include, but not be limited to, the following: employment, promotion, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training including apprenticeship.

C. The Contractor agrees that no qualified handicapped person shall, on the basis of handicap, be excluded from participation or be denied the benefits of, or otherwise be subjected to discrimination under any program or activity of the Contractor. The Contractor further agrees to insert similar provisions in all subcontracts for services allowed under this Agreement under any program or activity.

D. The Contractor agrees to provide meaningful access to services for individuals with Limited English Proficiency (LEP) in accordance with Executive Order 13166, “Improving Access to Services for Persons with Limited English Proficiency.”

28. Findings and Sanctions

A. The Contractor agrees to be subject to the findings and sanctions assessed as a result of NMHIX audits, federal audits, and disallowances of the services provided pursuant to this Agreement and the administration thereof.

B. The Contractor will make repayment of any funds expended by NMHIX, subject to which an auditor with the jurisdiction and authority finds were expended, or to which appropriate federal funding agencies take exception and so request reimbursement through a disallowance or deferral based upon the acts or omissions of the Contractor that violate applicable federal statutes and/or regulations.

C. If NMHIX becomes aware of circumstances that might jeopardize continued federal funding, the situation shall be reviewed and reconciled by a mutually agreed upon panel of Contractor and NMHIX officials.

29. Federal Tax Information

A. Performance. In performance of this Agreement, and to the extent required by law, Contractor agrees to comply with and assume responsibility for compliance by Contractor's employees with the following requirements:

i. All work will be performed under the supervision of the Contractor or the Contractor's responsible employees.

ii. Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Agreement or as otherwise required by law. Inspection by or disclosure to anyone other than an officer or employee of the Contractor is prohibited.

iii. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

iv. No work involving returns and return information furnished under this Agreement will be subcontracted without ensuring compliance with appropriate safeguards.

v. The Contractor will maintain a list of employees authorized access. Such list will be provided to NMHIX and, upon request, to the IRS reviewing office.

vi. NMHIX will have the right to void the Agreement if the Contractor fails to provide the safeguards described above.

B. Criminal/Civil Sanctions for Disclosure of Protected Information. In performance of this Agreement, and to the extent required by law, Contractor agrees to the following requirements:

i. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five (5) years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by Internal Revenue Code (IRC) Sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

ii. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any returns or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Agreement. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any

person except as may be necessary in the performance of this Agreement. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as one (1) year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRC Sections 7213A and 7431.

iii. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to NMHIX records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

iv. Granting a Contractor access to Federal Tax Information (FTI) must be preceded by certifying that each individual understands NMHIX's security policy and procedures for safeguarding IRS information. The Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in NMHIX's files for review. As part of the certification and at least annually afterwards, contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A. The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches (See IRS Publication 1075, Tax Information Security Guidelines). For both the initial certification and the annual certification, the Contractor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements

30. Clean Air Act, Federal Water Pollution Control Act

Contractor shall comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act, 42 U.S.C. 7401 et seq., and the Federal Water Pollution Control Act, as amended 33 U.S.C. 1251 et seq..

31. Force Majeure

No party shall be deemed in default of, nor shall any party be liable for any damages suffered or costs incurred by another party arising out of any cessation, interruption, delay or failure to perform its obligations under this Agreement if such cessation, interruption, delay or failure results from causes beyond the party's reasonable control, including, without limitation, earthquake, flood, storm or other natural disaster, act of God,

acts of war, epidemics, acts of government, power failures, malicious network attacks, nuclear accidents, and acts of terrorism.

32. Insurance

A. The Contractor shall not begin the services required under this Agreement until it has: (a) obtained, and upon NMHIX's request provided to NMHIX, insurance certificates reflecting evidence of all insurance required herein; however, the NMHIX reserves the right to request, and the Contractor shall submit, copies of any policy upon reasonable request by NMHIX; (b) obtained NMHIX approval of each company or companies as required below; and (c) confirmed that all policies contain the specific provisions required. Contractor's liabilities, including but not limited to Contractor's indemnity obligations, under this Agreement, shall not be deemed limited in any way to the insurance coverage required herein. Maintenance of specified insurance coverage is a material element of this Agreement and Contractor's failure to maintain or renew coverage or to provide evidence of renewal during the term of this Agreement may be treated as a material breach of Agreement by NMHIX.
Further, the Contractor shall not modify any policy or endorsement thereto which increases NMHIX's exposure to loss for the duration of this Agreement.

B. Types of Insurance. At all times during the term of this Agreement, the Contractor shall maintain insurance coverage as follows:

(1) Commercial General Liability (CGL) Insurance must be written on an ISO Occurrence form or an equivalent form providing coverage at least as broad which shall cover liability arising from bodily injury, personal injury or property damage providing the following minimum limits of liability.

General Annual Aggregate (other than Products/Completed Operation)	$5,000,000
Products/Completed Operations Aggregate Limit	$5,000,000
Personal Injury Limit	$5,000,000
Each Occurrence	$5,000.000

(2) Automobile Liability. For all of the Contractor's automobiles including owned, hired and non-owned automobiles, the Contractor shall keep in full force and effect, automobile liability insurance providing coverage at least as broad for bodily injury and property damage with a combined single limit of not less than $5 million per accident. An insurance certificate shall be submitted to NMHIX that reflects coverage for any automobile.

(3) Professional Liability. For the Contractor and all of the Contractor's employees who are to perform professional services under this Agreement, the Contractor shall keep in full force and effect, Professional Liability insurance for any professional acts, errors or omissions. Such policy shall provide a limit of not less than $5,000,000 per claim and $5,000,000 annual aggregate. The Contractor shall ensure both that: (1) the policy retroactive date is on or before the date of commencement of the first work performed under this Agreement; and (2) the policy will be

maintained in force for a period of three years after substantial completion of the project or termination of this Agreement whichever occurs last. If professional services rendered under this Agreement include work relating to environmental or pollution hazards, the Contractors policy shall not contain exclusions for those activities.

(4) Workers' Compensation. For all of the Contractor's employees who are subject to this Agreement and to the extent required by any applicable state or federal law, the Contractor shall keep in full force and effect, a Workers' Compensation policy & Employers Liability policy. That policy shall provide

Employers Liability Limits as follows:

Bodily Injury by Accident	$5,000,000	Each Accident
Bodily Injury by Disease	$5,000,000	Each Employee
Bodily Injury by Disease	$5,000,000	Policy Limit

The Contractor shall provide an endorsement that the insurer waives the right of subrogation against NMHIX and its respective officials, officers, employees, agents, volunteers and representatives.

C. Cancellation. Except as provided for under New Mexico law, all policies of insurance required hereunder must provide that the NMHIX is entitled to thirty (30) days prior written notice (10 days for cancellation due to non-payment of premium) of cancellation or non-renewal of the policy or policies. Cancellation provisions in insurance certificates shall not contain the qualifying words “endeavor to” and “but failure to mail such notice shall impose no obligation or liability of any kind upon the company, its agents or representatives”. In the event the Contractors’ insurance carriers will not agree to this notice requirement, the Contractor will provide written notice to the NMHIX within four working days of Contractors receipt of notice from its insurance carrier(s) of any cancellation, nonrenewal or material reduction of the required insurance.

D. Insurer Requirements. All insurance required by express provision of this Agreement shall be carried only by responsible insurance companies that have rated “A-” and “V” or better by the A.M. Best Key Rating Guide, that are authorized to do business in the State of New Mexico, and that have been approved by the NMHIX. The NMHIX will accept insurance provided by non-admitted, “surplus lines” carriers only if the carrier is authorized to do business in the State of New Mexico.

E. Deductibles. All deductibles or co-payments on any policy shall be the responsibility of the Contractor.

F. Specific Provisions Required. Each policy shall expressly provide, and an endorsement shall be submitted to the NMHIX, that the policy or policies providing coverage for Commercial General Liability must be endorsed to include as an Additional Insured, the NMHIX and its respective officials, officers, employees, agents, volunteers and representatives.

G. All policies required herein are primary and non-contributory to any insurance that may be carried by the NMHIX and its officials, officers, employees, agents, volunteers and representatives, as reflected in an endorsement which shall be submitted to the NMHIX.

H. The Contractor agrees that for the time period defined above, there will be no changes or endorsements to the policy that increase the NMHIX's exposure to loss.

I. Before performing any Professional Services, the Contractor shall provide the NMHIX with all Certificates of Insurance accompanied with all endorsements.

J. The NMHIX reserves the right, from time to time, to review the Contractor's insurance coverage, limits, and deductible and self-insured retentions to determine if they are acceptable to the NMHIX. The NMHIX will reimburse the Contractor for the cost of the additional premium for any coverage requested by the NMHIX in excess of that required by this Agreement without overhead, profit, or any other markup.

K. The Contractor may obtain additional insurance not required by this Agreement.

33. New Mexico Tort Claims Act

Any liability incurred by NMHIX in connection with this Agreement is subject to the immunities and limitations of the New Mexico Tort Claims Act, NMSA 1978, § 41-4-1, *et seq.*, as amended. NMHIX and its "public employees" as defined in the New Mexico Tort Claims Act, do not waive sovereign immunity, do not waive any defense, and do not waive any limitation of liability pursuant to law. No provision in this Agreement modifies or waives any provision of the New Mexico Tort Claims Act.

34. Communications

The NMHIX desires to maintain a consistent and coherent public message regarding the work of the NMHIX, its contracting partners, and the contractual relationship between the NMHIX and its contracting partners. Contractor expressly acknowledges the NMHIX's interest in this regard and agrees that Contractor shall not communicate with the media or the public regarding this Agreement or the work performed pursuant to this Agreement, during the term of the Agreement and for a reasonable period of time following the termination of this Agreement, without requesting and receiving authorization from the NMHIX to engage in the communications. Contractor also agrees to comply with the NMHIX Communications Policy, as it may be amended from time to time.

35. Compliance with Law

The Contractor agrees to comply with all laws and regulations that are applicable to this Agreement and the Contractor's Scope of Work now enacted or that become effective during the term of this Agreement, including but not limited to, laws and regulations enacted pursuant to the Affordable Health Care Act.

36. Counterparts

This Agreement may be executed in counterparts, each of which shall constitute an original.

IN WITNESS WHEREOF, **the parties have executed this Agreement as of the date of the signatures below.**

_____ _____

Amy Dowd, NMHIX CEO Date

_____ _____

Contractor Date

EXHIBIT A
Scope of Work

Exhibit B

Privacy and Security Standards

Definitions. Capitalized terms not otherwise specifically defined in this specific term and condition shall have the meaning set forth in Section B.

Authorized Functions. Contractor may collect, handle, disclose, access, maintain, store, and/or use PII of Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees, or from these individuals' legal representative(s) or Authorized Representative(s), only to perform the required duties described in section 1311(i)(3) of the Affordable Care Act, 45 CFR 155.210(e), the Cooperative Agreement to Support Navigators in Federally-Facilitated and State Partnership Exchanges Funding Opportunity Announcement ("Navigator FOA"), and45 CFR 155.215(a)(1)(iii), as well as in Contractor's approved work and project plans.

The required duties that will most likely involve the collection, handling, disclosure, access, maintenance, storage and/or use of PII of Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees, or from these individuals' legal representatives(s) or Authorized Representatives, include the following:

- Provide information and services in a fair, accurate, and impartial manner. Such information must acknowledge other health programs such as Medicaid and CHIP;
- Facilitate selection of a QHP;
- Provide referrals to any applicable office of health insurance consumer assistance or health insurance ombudsman established under Section 2793 of the PHS Act, or any other appropriate State agency or agencies, for any enrollee with a grievance, complaint, or question regarding their health plan, coverage, or a determination under such plan or coverage; and
- Provide information in a manner that is culturally and linguistically appropriate to the needs of the population being served by the Exchange, including individuals with limited English proficiency, and ensure accessibility and usability of Health care guide tools and functions for individuals with disabilities in accordance with the Americans with Disabilities Act and Section 504 of the Rehabilitation Act.

Such information may not be reused for any other purpose.

Other Required Duties: Contractor must also maintain expertise in eligibility, enrollment, and program specifications and conduct public education activities to raise awareness about the Exchange; however, it is not expected or required that Contractor collect, handle, disclose, access, maintain, store and/or use PII of Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees, or from these individuals' legal representatives(s) or Authorized Representatives for this function. To the extent that Contractor does so, it must comply with all of the provisions of this specific term and condition, as well as Sections A and B that apply to Contractor's activities.

PII Received. Subject to the terms and conditions of this Agreement and applicable laws, in performing the tasks contemplated under this Agreement, Contractor may create, collect, disclose, access, maintain, store, and/or use the following PII from Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees, or from these individuals' legal representative(s) or Authorized Representative(s):

APTC percentage and amount applied
Auto disenrollment information
Applicant Name
Applicant Address
Applicant Birthdate
Applicant Telephone number
Applicant Email
Applicant spoken and written language preference
Applicant Medicaid Eligibility indicator, start and end dates
Applicant Children's Health Insurance Program eligibility indicator, start and end dates
Applicant QHP eligibility indicator, start and end dates
Applicant APTC percentage and amount applied eligibility indicator, start and end dates
Applicant household income
Applicant Maximum APTC amount
Applicant CSR eligibility indicator, start and end dates
Applicant CSR level
Applicant QHP eligibility status change
Applicant APTC eligibility status change
Applicant CSR eligibility status change
Applicant Initial or Annual Open Enrollment Indicator, start and end dates
Applicant Special Enrollment Period eligibility indicator and reason code
Contact Name
Contact Address
Contact Birthdate
Contact Telephone number
Contact Email
Contact spoken and written language preference
Enrollment group history (past six months)
Enrollment type period
FFE Applicant ID
FFE Member ID
Issuer Member ID
Net premium amount
Premium Amount, start and end dates
Pregnancy status indicator
PII related to any enrollee with a grievance, complaint, or question regarding their health plan, coverage, or a determination as described in 45 CFR §155.210(e)(4)
Special enrollment period reason
Subscriber Indicator and relationship to subscriber
Social Security Number
Tobacco use indicator and last date of tobacco

Storing PII. Contractor is not expected or required to maintain or store any of the above listed PII as a result of carrying out the Authorized Functions described above or any other required duties, other than in connection with the storage of consent forms required by this specific term and condition. To the extent that Contractor does maintain or store information, it must comply with all of the provisions of this specific term and condition and Sections A and B that address maintenance or storage of PII.

Privacy and Security Obligations of Contractor. As a condition of this contract, Contractor will

implement and comply with all Exchange privacy and security standards set forth in this specific term and condition as well as Sections A and B, and the Minimum Acceptable Risk Standards for Exchanges (MARS-E) , which is available at http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/Minimum-Acceptable-Risk-Standards-for-Exchanges-ERA-Supp-v-1-0-08012012-a.pdf .

Consent Form. Prior to collecting any PII, Contractor must obtain the consent of Consumers, Applicants, Qualified Individuals, Qualified Employers, Qualified Employees, or Enrollees or these individuals' legal representative(s) or Authorized Representative(s) to assist them with the Marketplace eligibility and enrollment process or other post-enrollment assistance. A template consent form has been provided separately to all Contractors.

Applicability to Workforce. Contractor must impose the same standards described in this specific term and condition and in Sections A and B on all Workforce members, including subcontractors, working with the Contractor on this contract program.

Survival. Contractor covenants and agrees to destroy all PII of Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or those individuals' legal representatives or Authorized Representatives in its possession at the end of the record retention period required under this specific term and condition and Sections A and B. If, upon the termination or expiration of this contract, the Health care guide has in its possession PII for which no retention period is specified in this specific term and condition and/or Sections A and B, such PII shall be destroyed within 30 Days of the termination or expiration of this contract. Contractor's duty to protect and maintain the privacy and security of PII, as provided for in accordance with this specific term and condition, and Sections A and B, shall continue in full force and effect until such PII is destroyed and shall survive the termination or withdrawal of the Health care guide Contractor and/or expiration of this Agreement.

Section A: Special Terms and Conditions

PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS FOR NON-EXCHANGE ENTITIES

Statement of Applicability:

These standards and implementation specifications are established in accordance with Section 1411(g) of the Affordable Care Act (42 U.S.C. § 18081(g)) and 45 CFR 155.260. All terms used herein carry the meanings assigned in Section B, which is also included in this document.

The standards and implementation specifications that are set forth in this Section A and Version 1.0 of the MARS-E suite of documents (which can be found at http://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/) are the same as, or more stringent than, the privacy and security standards and implementation specifications that have been established for the Federally-Facilitated Exchanges ("FFEs") under Section 1321(c) of the Affordable Care Act (42 U.S.C. § 18041(c)).

The New Mexico Health Insurance Exchange (NMHIX) will enter into contracts (hereinafter "Agreement" or "Agreements") with Non-Exchange Entities that gain access to Personally Identifiable Information ("PII") exchanged with the FFE and NMHIX, or directly from Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representatives or Authorized Representatives. That Agreement including this Section A, govern any PII that is created, collected, disclosed, accessed, maintained, stored, or used by Non-Exchange Entities in the context of the FFE. In signing that Agreement, in which this Section A has been incorporated, Non-Exchange Entities agree to comply with the standards and implementation specifications laid out in this

document and the referenced MARS-E suite of documents while performing the Authorized Functions outlined in their respective Agreements.

NON-EXCHANGE ENTITY PRIVACY AND SECURITY STANDARDS AND IMPLEMENTATION SPECIFICATIONS

In addition to the standards and implementation specifications set forth in the MARS-E suite of documents noted above, Non-Exchange Entities must meet the following privacy and security standards and implementation specifications to the extent they are not inconsistent with any applicable MARS-E standards.

(1) *Individual Access to PII: In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities that maintain and/or store PII must provide Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representatives and Authorized Representatives, with a simple and timely means of appropriately accessing PII pertaining to them and/or the person they represent in a physical or electronic readable form and format.*

a. Standard: Non-Exchange Entities that maintain and/or store PII must implement policies and procedures that provide access to PII upon request.

i. Implementation Specifications:

1. Access rights must apply to any PII that is created, collected, disclosed, accessed, maintained, stored, and used by the Non-Exchange Entity to perform any of the Authorized Functions outlined in their respective agreements with the NMHIX.
2. The release of electronic documents containing PII through any electronic means of communication (e.g., e-mail, web portal) must meet the verification requirements for the release of "written documents" in Section (5)b below.
3. Persons legally authorized to act on behalf of the Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers regarding their PII, including individuals acting under an appropriate power of attorney that complies with applicable state and federal law, must be granted access in accordance with their legal authority. Such access would generally be expected to be coextensive with the degree of access available to the Subject Individual.
4. At the time the request is made, the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employees, Qualified Employers, or these individuals' legal representatives or Authorized Representatives should generally be required to specify which PII he or she would like access to. The Non-Exchange Entity may assist them in determining their Information or data needs if such assistance is requested.
5. Subject to paragraphs (1) a.i.6 and 7 below, Non-Exchange Entities generally must provide access to the PII in the form or format requested, if it is readily producible in such form or format.
6. The Non-Exchange Entity may charge a fee only to recoup their costs for labor for copying the PII, supplies for creating a paper copy or a copy on electronic media, postage if the PII is mailed, or any costs for preparing an

explanation or summary of the PII if the contractors has requested and/or agreed to receive such summary. If such fees are paid, the Non-Exchange Entity must provide the requested copies in accordance with any other applicable standards and implementation specifications.

7. A Non-Exchange Entity that receives a request for notification of, or access to PII must verify the requestor's identity in accordance with Section (5)b.
8. A Non-Exchange Entity must complete its review of a request for access or notification (and grant or deny said notification and/or access) within 30 days of receipt of the notification and/or access request.
9. Except as otherwise provided in (1)a.i.10, if the requested PII cannot be produced, the Non-Exchange Entity must provide an explanation for its denial of the notification or access request, and, if applicable, information regarding the availability of any appeal procedures, including the appropriate appeal authority's name, title, and contact information.
10. Unreviewable grounds for denial. Non-Exchange Entities may deny access to PII that they maintain or store without providing an opportunity for review, in the following circumstances:
    a. If the PII was obtained or created solely for use in legal proceedings;
    b. If the PII is contained in records that are subject to a law that either permits withholding the PII or bars the release of such PII.

(2) *Openness and Transparency*. *In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities must ensure openness and transparency about policies, procedures, and technologies that directly affect Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employers, and Qualified Employees, and their PII.*

a. Standard: Privacy Notice Statement. Prior to collecting PII, the Non-Exchange Entity must provide a notice that is prominently and conspicuously displayed on a public facing Web site, if applicable, or on the electronic and/or paper form the Non-Exchange Entity will use to gather and/or request PII.

    i. Implementation Specifications.
        1. The statement must be written in plain language and provided in a manner that is accessible and timely to people living with disabilities and with limited English proficiency.
        2. The statement must contain at a minimum the following information:
            a. Legal authority to collect PII;
            b. Purpose of the information collection;
            c. To whom PII might be disclosed, and for what purposes;
            d. Authorized uses and disclosures of any collected information;
            e. Whether the request to collect PII is voluntary or mandatory under the applicable law;
            f. Effects of non-disclosure if an individual chooses not to provide the requested information.

3. The Non-Exchange Entity shall maintain its Privacy Notice Statement content by reviewing and revising as necessary on an annual basis, at a minimum, and before or as soon as possible after any change to its privacy policies and procedures.
4. If the Non-Exchange Entity operates a Web site, it shall ensure that descriptions of its privacy and security practices, and information on how to file complaints with NMHIX and the Non-Exchange Entity, are publicly available through its Web site.

(3) <u>*Individual choice.*</u> *In keeping with the standards and implementation specifications used by the FFE, Non-Exchange Entities should ensure that Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representatives or Authorized Representatives, are provided a reasonable opportunity and capability to make informed decisions about the creation, collection, disclosure, access, maintenance, storage, and use of their PII.*

a. <u>Standard: Informed Consent</u>. The Non-Exchange Entity may create, collect, disclose, access, maintain, store, and use PII from Consumers, Applicants, Qualified Individuals, Enrollees, or these individuals' legal representatives or Authorized Representatives, only for the functions and purposes listed in the Privacy Notice Statement and any relevant agreements in effect as of the time the information is collected, unless the NMHIX, the FFE or Non-Exchange Entity obtains informed consent from such individuals.

i. <u>Implementation specifications:</u>
1. The Non-Exchange Entity must obtain informed consent from individuals for any use or disclosure of information that is not permissible within the scope of the Privacy Notice Statement and any relevant agreements that were in effect as of the time the PII was collected. Such consent must be subject to a right of revocation.
2. Any such consent that serves as the basis of a use or disclosure must:
    a. Be provided in specific terms and in plain language;
    b. Identify the entity collecting or using the PII, and/or making the disclosure;
    c. Identify the specific collections, use(s), and disclosure(s) of specified PII with respect to a specific contractor(s);
    d. Provide notice of an individual's ability to revoke the consent at any time.
3. Consent documents must be appropriately secured and retained for 10 years.

(4) <u>*Creation, collection, disclosure, access, maintenance, storage, and use limitations.*</u> *In keeping with the standards and implementation specifications used by the NMHIX and by the FFE, Non-Exchange Entities must ensure that PII is only created, collected, disclosed, accessed, maintained, stored, and used, to the extent necessary to accomplish a specified purpose(s) in the Agreement and any appendices. Such information shall never be used to discriminate against a Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, or Qualified Employer.*

a. Standard: Other than in accordance with the consent procedures outlined above, the Non-Exchange Entity shall only create, collect, disclose, access, maintain, store, and use PII:
    1. To the extent necessary to ensure the efficient operation of the Exchange;
    2. In accordance with its published Privacy Notice Statement and any applicable agreements that were in effect at the time the PII was collected, including the consent procedures outlined above in Section (3) above; and/or
    3. In accordance with the permissible functions outlined in the regulations and agreements between NMHIX and the Non-Exchange Entity.

b. Standard: Non-discrimination. The Non-Exchange Entity should, to the greatest extent practicable, collect PII directly from the Consumer, Applicant, Qualified Individual, Enrollee, Qualified Employee, or Qualified Employer, when the information may result in adverse determinations about benefits.

c. Standard: Prohibited uses and disclosures of PII

    i. Implementation Specifications:

        1. The Non-Exchange Entity shall not request Information regarding citizenship, status as a national, or immigration status for an individual who is not seeking coverage for himself or herself on any application.
        2. The Non-Exchange Entity shall not require an individual who is not seeking coverage for himself or herself to provide a social security number (SSN), except if an Applicant's eligibility is reliant on a tax filer's tax return and their SSN is relevant to verification of household income and family size.
        3. The Non-Exchange Entity shall not use PII to discriminate, including employing marketing practices or benefit designs that will have the effect of discouraging the enrollment of individuals with significant health needs in QHPs.

(5) *Data quality and integrity. In keeping with the standards and implementation specifications used by NMHIX and by the FFE, Non-Exchange Entities should take reasonable steps to ensure that PII is complete, accurate, and up-to-date to the extent such data is necessary for the Non-Exchange Entity's intended use of such data, and that such data has not been altered or destroyed in an unauthorized manner, thereby ensuring the confidentiality, integrity, and availability of PII.*

a. Standard: Right to Amend, Correct, Substitute, or Delete PII. In keeping with the standards and implementation specifications used by NMHIX and by the FFE, Non-Exchange Entities must offer Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, and Qualified Employers, or these individuals' legal representatives or Authorized Representatives, an opportunity to request amendment, correction, substitution, or deletion of PII maintained and/or stored by the Non-Exchange Entity if such individual believes that the PII is not accurate, timely, complete, relevant, or necessary to accomplish an Exchange-

related function, except where the Information questioned originated from other sources, in which case the individual should contact the originating source.

i. Implementation Specifications:

1. Such individuals shall be provided with instructions as to how they should address their requests to the Non-Exchange Entity's Responsible Official, in writing or telephonically. They may also be offered an opportunity to meet with such individual or their delegate(s) in person.
2. Such individuals shall be instructed to specify the following in each request:
    a. The PII they wish to correct, amend, substitute or delete;
    b. The reasons for requesting such correction, amendment, substitution, or deletion, along with any supporting justification or evidence.
3. Such requests must be contracted or denied within no more than 10 working days of receipt.
4. If the Responsible Official (or their delegate) reviews these materials and ultimately agrees that the identified PII is not accurate, timely, complete, relevant or necessary to accomplish the function for which the PII was obtained/provided, the PII should be corrected, amended, substituted, or deleted in accordance with applicable law.
5. If the Responsible Official (or their delegate) reviews these materials and ultimately does not agree that the PII should be corrected, amended, substituted, or deleted, the requestor shall be informed in writing of the denial, and, if applicable, the availability of any appeal procedures. If available, the notification must identify the appropriate appeal authority including that authority's name, title, and contact information.

b. Standard: Verification of Identity for Requests to Amend, Correct, Substitute or Delete PII. In keeping with the standards and implementation specifications used by the NMHIX and the FFE, Non-Exchange Entities that maintain and/or store PII must develop and implement policies and procedures to verify the identity of any person who requests access to; notification of; or amendment, correction, substitution, or deletion of PII that is maintained by or for the Non-Exchange Entity. This includes confirmation of an individuals' legal or personal authority to access; receive notification of; or seek amendment, correction, substitution, or deletion of a Consumer's, Applicant's, Qualified Individuals', Enrollee's, Qualified Employee's, or Qualified Employer's PII.

i. Implementation Specifications:

1. The requester must submit through mail, via an electronic upload process, or in-person to the Non-Exchange Entity's Responsible Official, a copy of one of the following government-issued identification: a driver's license, school identification card, voter registration card, U.S. military card or draft record, identification card issued by the federal, state or local government,

including a U.S. passport, military dependent's identification card, Native American tribal document, or U.S. Coast Guard Merchant Mariner card.

2. If such requester cannot provide a copy of one of these documents, he or she can submit two of the following documents that corroborate one another: a birth certificate, Social Security card, marriage certificate, divorce decree, employer identification card, high school or college diploma, and/or property deed or title.

c. Standard: Accounting for Disclosures. Except for those disclosures made to the Non-Exchange Entity's Workforce, or sub-contractor, who have a need for the record in the performance of their duties; and the disclosures that are necessary to carry out the required functions of the Non-Exchange Entity, Non-Exchange Entities that maintain and/or store PII shall maintain an accounting of any and all disclosures.

i. Implementation Specifications:

1. The accounting shall contain the date, nature, and purpose of such disclosures, and the name and address of the person or agency to whom the disclosure is made
2. The accounting shall be retained for at least 10 years after the disclosure, or the life of the record, whichever is longer.
3. Notwithstanding exceptions in Section (1)a.10, this accounting shall be available to Consumers, Applicants, Qualified Individuals, Enrollees, Qualified Employees, Qualified Employers, or these individuals' legal representatives or Authorized Representatives, on their request per the procedures outlined under the access standards in Section (1) above.

(6) *Accountability. In keeping with the standards and implementation specifications used by the FEE, Non-Exchange Entities should adopt and implement the standards and implementation specifications in this document and the cited MARS-E document suite, in a manner that ensures appropriate monitoring and other means and methods to identify and report Incidents and/or Breaches.*

a. Standard: Reporting. The Non-Exchange Entity must implement Breach and Incident handling procedures that are consistent with CMS' Incident and Breach Notification Procedures[1] and memorialized in the Non-Exchange Entity's own written policies and procedures. Such policies and procedures would:

i. Identify the Non-Exchange Entity's Designated Privacy Official, if applicable, and/or identify other personnel authorized to access PII and responsible for reporting and managing Incidents or Breaches to CMS.

ii. Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches, which should include information regarding the potential need for CMS to immediately suspend or revoke access to the Hub for containment purposes; and

[1] Available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_7-1_Incident_Handling_Standard.pdf

iii. Require reporting any Incident or Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within required time frames.

b. Standard: Standard Operating Procedures. The Non-Exchange Entity shall incorporate privacy and security standards and implementation specifications, where appropriate, in its standard operating procedures that are associated with functions involving the creation, collection, disclosure, access, maintenance, storage, or use of PII.

i. Implementation Specifications:

1. The privacy and security standards and implementation specifications shall be written in plain language and shall be available to all of the Non-Exchange Entity's Workforce members, or sub-contractors, whose responsibilities entail the creation, collection, maintenance, storage, access, or use of PII.
2. The procedures shall ensure the Non-Exchange Entity's cooperation with CMS in resolving any Incident or Breach, including (if requested by CMS) the return or destruction of any PII files it received under the Agreement; the provision of a formal response to an allegation of unauthorized PII use, reuse or disclosure; and/or the submission of a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures.
3. The standard operating procedures must be designed and implemented to ensure the Non-Exchange Entity and its Workforce, or sub-contractor, comply with the standards and implementation specifications contained herein, and must be reasonably designed, taking into account the size and the type of activities that relate to PII undertaken by the Non-Exchange Entity, to ensure such compliance.

a. Standard: Training and Awareness. The Non-Exchange Entity shall develop training and awareness programs for members of its Workforce that create, collect, disclose, access, maintain, store, and use PII while carrying out any Authorized Functions.

i. Implementation Specifications:

1. The Non-Exchange Entity must require such individuals to successfully complete privacy and security training, as appropriate for their work duties and level of exposure to PII, prior to when they assume responsibility for/have access to PII.
2. The Non-Exchange Entity must require periodic role-based training on an annual basis, at a minimum.
3. The successful completion by such individuals of applicable training programs, curricula, and examinations offered through the FFE is sufficient to satisfy the requirements of this paragraph.

b. Standard: Security Controls. The FFE shall adopt and implement the Security Control standards cited in the MARS-E document suite for protecting the confidentiality, integrity, and availability of PII.

i. Implementation Specifications:

1. Implementation specifications for each Security Control are provided in the MARS-E document suite.

Section B: Special Terms and Conditions

DEFINITIONS

(1) **Affordable Care Act (ACA)** means the Patient Protection and Affordable Care Act (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), which are referred to collectively as the Affordable Care Act.

(2) **Access** means availability of a SORN Record to a subject individual.

(3) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 CFR 155.20.

(4) **Applicant** has the meaning set forth in 45 CFR 155.20.

(5) **Authorized Function** means a task performed by a Non-Exchange Entity that the Non-Exchange Entity is explicitly authorized or required to perform based on applicable law or regulation, and as enumerated in Attachment B of the Special Terms and Conditions that incorporates this Attachment.

(6) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 CFR 155.227.

(7) **Breach** is defined by OMB Memorandum M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information (May 22, 2007), as the compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, loss of control or any similar term or phrase that refers to situations where persons other than authorized users or for an other than authorized purpose have access or potential access to Personally Identifiable Information (PII), whether physical or electronic.

(8) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (CMS).

(9) **CMS** means the Centers for Medicare & Medicaid Services.

(10) **CMS Data Services Hub (Hub)** is the CMS Federally-managed service to interface data among connecting entities, including HHS, certain other Federal agencies, and State Medicaid agencies.

(11) **Consumer** means a person who, for himself or herself, or on behalf of another individual, seeks information related to eligibility or coverage through a Qualified Health Plan **(**QHP) or other Insurance Affordability Program, or whom an agent or broker (including Web-brokers), Health care guide, Issuer, Certified Application Counselor, or other entity assists in applying for a coverage through QHP, applying for APTCs and CSRs, and/or completing enrollment in a QHP through its web site for individual market coverage.

(12) **Cost-sharing Reduction (CSR)** has the meaning set forth in 45 CFR 155.20.

(13) **Day or Days** means calendar days unless otherwise expressly indicated in the relevant provision of the Notice of Award terms and conditions that incorporates this Section B.

(14) **Designated Privacy Official** means a contact person or office responsible for receiving complaints related to Breaches or Incidents, able to provide further information about matters covered by the notice, responsible for the development and implementation of the privacy and security policies and procedures of the Non-Exchange Entity, and ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the privacy and security of PII.

(15) **Enrollee** has the meaning set forth in 45 CFR 155.20.

(16) **Exchange** has the meaning set forth in 45 CFR 155.20.

(17) **Federally-facilitated Exchange (FFE)** means an **Exchange** (or **Marketplace**) established by HHS and operated by CMS under Section 1321(c)(1) of the ACA for individual or small group market coverage, including the Federally-facilitated Small Business Health Options Program (**FF-SHOP**). **Federally-facilitated Marketplace (FFM)** has the same meaning as FFE. The FFE is serving as the individual exchange in New Mexico for 2015.

(18) **Health Insurance Coverage** has the meaning set forth in 45 CFR 155.20.

(19) **HHS** means the U.S. Department of Health & Human Services.

(20) **Incident**, or **Security Incident**, means the act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

(21) **Information** means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

(22) **Issuer** has the meaning set forth in 45 CFR 144.103.

(23) **Minimum Acceptable Risk Standards—Exchanges (MARS-E)** means a CMS-published suite of documents, version 1.0 (August 1, 2012), that defines the security standards required pursuant to 45 CFR 155.260 and 45 CFR 155.270, for any Exchange, individual, or entity gaining access to information submitted to an Exchange or through an Exchange using a direct, system-to-system connection to the Hub, available on the CCIIO web site.

(24) **Health care guide** has the meaning set forth under "Navigator" in 45 CFR 155.20.

(25) **Non-Exchange Entity** has the meaning at 45 CFR 155.260(b), and includes but is not limited to Health care guides.

(26) **OMB** means the Office of Management and Budget.

(27) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-07-16 (May 22, 2007) and means information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, *etc.*, alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

(28) **Qualified Employee** has the meaning set forth in 45 CFR 155.20.

(29) **Qualified Employer** has the meaning set forth in 45 CFR 155.20.

(30) **Qualified Health Plan (QHP)** has the meaning set forth in 45 CFR 155.20.

(31) **Qualified Individual** has the meaning set forth in 45 CFR 155.20.

(32) **Responsible Official** means an individual or officer responsible for managing a Non-Exchange Entity or Exchange's records or information systems, or another individual designated as an individual to whom requests can be made, or the designee of either such officer or individual who is

listed in a Federal System of Records Notice as the system manager, or another individual listed as an individual to whom requests may be made, or the designee of either such officer or individual.

(33) **Security Control** means a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

(34) **State** means the State where the Health care guide that is a party to the contract is operating.

(35) **State Partnership Exchange** means a type of FFE in which a State assumes responsibility for carrying out certain activities related to plan management, consumer assistance, or both.

(36) **Subject Individual** means that individual to whom a SORN Record pertains.

(37) **System of Records Notice (SORN)** means a notice published in the Federal Register notifying the public of a System of Records maintained by a Federal agency. The notice describes privacy considerations that have been addressed in implementing the system.

(38) **Workforce** means a Non-Exchange Entity's or FFE's employees, agents, contractors, subcontractors, officers, directors, agents, representatives, volunteers and any other individual who may create, collect, disclose, access, maintain, store, or use PII in the performance of his or her duties.