Medicaid Management Information System Replacement (MMISR) Project

Security 1: Security Approach

NM HSD Deliverable Owner: Sean Pearson
System Integrator (SI) Deliverable Owner: Tonya Love
Configuration Number v1.0
January 18, 2019
# Table of Contents

1. **Introduction** ................................................................................................................. 1  
   1.1 Overview .................................................................................................................. 1  
   1.2 Purpose .................................................................................................................... 1  

2. **Security Approach** ........................................................................................................ 2  
   2.1 Security Planning Policy Procedures ........................................................................... 2  
   2.2 Minimum Acceptable Risk Standards for Exchanges .................................................. 8  
   2.3 PL-1 and PM-1 Controls .............................................................................................. 8  
   2.4 Security Artifacts ....................................................................................................... 9  
   2.5 Security Control Assessments .................................................................................... 10  
   2.6 Security Activities ..................................................................................................... 11  

3. **Team Members** ............................................................................................................. 14  
   3.1 Certification and Accreditation Team ......................................................................... 14  
   3.2 Security Team ........................................................................................................... 15  

4. **System Categorization** .................................................................................................. 16  
   4.1 MMISR Modules ....................................................................................................... 16  
   4.2 Integration Platform Components .............................................................................. 17  
   4.3 Interconnected Systems ............................................................................................ 17  

5. **Programmatic Activities** ............................................................................................... 17  
   5.1 Team Training ............................................................................................................ 17  
   5.2 Configuration Management ...................................................................................... 18  
   5.3 Risk Management ...................................................................................................... 18  
   5.4 Change Management .................................................................................................. 19  

6. **CMS Certification** ......................................................................................................... 19  

7. **Assumptions, Constraints, and Risks** ........................................................................... 19  
   7.1 Assumptions ............................................................................................................... 19  
   7.2 Constraints ................................................................................................................ 20  
   7.3 Risks .......................................................................................................................... 20  

8. **Requirements Traceability** ........................................................................................... 20
9. Appendices.......................................................................................................................... 21
  9.1 Appendix A: Record of Changes......................................................................................... 21
  9.2 Appendix B: List of Acronyms .......................................................................................... 21
  9.3 Appendix C: Glossary.......................................................................................................... 24
  9.4 Appendix D: Table Description of Information for MMISR Modules and Components .......................................................................................................................... 25
  9.5 Appendix E: MECT Checklist............................................................................................ 27
  9.6 Appendix F: RACI CHART.................................................................................................. 27

List of Figures
Figure 1 Integrating Security into the SDLC................................................................................ 2

List of Tables
Table 1: Certification and Accreditation Team (C&A)................................................................ 14
Table 2: Security Team Roles and Responsibilities.................................................................... 15
Table 3: Role Matrix .................................................................................................................. 16
Table 4: Deliverable Record of Changes.................................................................................... 21
Table 5: List of Acronyms.......................................................................................................... 21
Table 6: Glossary........................................................................................................................ 24
Table 7: MMISR Modules and Components Information.......................................................... 25
Table 8: MECT Checklist........................................................................................................... 27
Table 9 MMISR Roles and Responsibilities RACI Chart.......................................................... 27
Table 10: Business Process Outsourcing Contractor Specific.................................................... 28
1. Introduction

The Security Approach describes the methodology for developing the security standards that will apply across the Department of Health and Human Services (HHS) 2020 enterprise. This document also provides a comprehensive description of how the System Integrator (SI) Contractor will implement and carry out this over-arching approach to enterprise security.

1.1 Overview

The New Mexico Human Services Department (NM HSD) has adopted the Health and Human Services (HHS) 2020 vision, a transformational, enterprise approach to the health and human services business. HHS 2020 will move service delivery from a program-centric approach to a stakeholder-centric approach. NM HSD will migrate away from program and technology silos into an integrated, flexible framework that supports service delivery and stakeholder interaction across HHS programs and organizations. HHS 2020 is technology-enabled but includes rethinking the organizational design, redesigning, and streamlining business processes, and reducing barriers between organizations within the HHS enterprise.

Please see “Section 1: Introduction” in the Project Management Plan for a detailed MMISR overview.

1.2 Purpose

The Security Approach identifies security best practices and applicable security controls for the HHS 2020 enterprise systems, as well as outlining an overarching security framework. This document addresses the following:

- The procedures to implement the security planning policy.
- The Minimum Acceptable Risk Standards for Exchanges (MARS-E) Version 2.0 (v2.0) Planning-1 (PL-1) and Program Management-1 (PM-1) control sets, which are part of the Centers for Medicare and Medicaid (CMS) approved MARS-E v2.0 suite of security controls.
- Implementation of security compliance and governance policies.

This document will ensure that all HHS 2020 enterprise stakeholders are aware of the security standards that are established and requirements set forth in the PL-1 and PM-1 control families.
2. Security Approach

The Security Approach provides an overarching security structure for the HHS 2020. The security planning policy and associated security planning controls that are applicable across the HHS 2020 enterprise follow the MARS-E v2.0 and PM-1 control.

This approach integrates security into each phase of the System Development Life Cycle (SDLC). By doing so, it will identify and mitigate security risks in the early stages of development and facilitate certification efforts later in the project life cycle. Deliverables and/or activities required in each phase of the SDLC must be approved and have signoff from NM HSD where applicable.

Figure 1 demonstrates a sample of security deliverables being integrated into the SDLC process.

Figure 1 Integrating Security into the SDLC

SDLC Process

Secure SDLC Process

2.1 Security Planning Policy Procedures

The SI Contractor security team will implement the NM HSD Security Planning Policy procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in accordance with the MARS-E v2.0 and other federal and State laws and directives.

The planning will establish the MARS-E v2.0 as the required set of controls that must be implemented to protect the data that is used, maintained, exchanged, and stored throughout the HHS 2020 enterprise.

In accordance with planning, all HHS 2020 enterprise systems will be required to integrate security into each phase of the system development life cycle. The following sections outline each phase of the SDLC and describe the activities by which security must be integrated.

2.1.1 Requirements

The requirements phase is used to clearly define and document the product requirements. The sections below define how security will be integrated into this phase. Early involvement helps the developers and architects understand the security requirements from the initial stages.
2.1.1.1 Identification of Security Policies Followed by NM HSD

The SI Contractor security team will review the security policies that NM HSD currently follows. They will:

1. Contact the NM HSD Chief Information Security Officer (CISO) for the location of the security policies.
2. Analyze the policies and standards NM HSD currently follows.
3. A gap analysis will be performed by the SI Contractor team to ensure current policies are in line with the MARS-E v2.0. Deficiencies will be provided in a report to the NM HSD team and plan to update policies as needed will be devised and implemented.

2.1.1.2 Development of Requirements

To ensure that security requirements are captured during the requirements phase, the following steps will be exercised:

1. The Security Analyst will review the administrative, operational and technical controls with the Business Analyst (BA) to determine which controls are applicable to each work stream. This determination will be based upon the functionality of the workstream and the type of data that is collected, used, processed, or stored within that workstream.
2. Based on the selection of the appropriate control families, the security analyst will determine which controls are inherited/common controls (controls that will be used by the system but are implemented by another entity) or hybrid controls (controls that are partially implemented by the system and partially implemented by another entity).
3. Based on the selection of the appropriate control families, the security analyst will determine if there are any specific controls that are not applicable.
4. Once inherited controls, and N/A controls have been updated in the System Security Plan (SSP), the security team will begin working with the requirements team/BA to implement the applicable operational, and technical controls for each applicable control family. Each applicable control must translate into a requirement to ensure the control has been implemented. For example, control SC-28 states, “The information system protects the confidentiality and integrity of information at rest.” The requirement may read as, “The system must employ Federal Information Processing Standards (FIPS) 140-2 compliant encryption modules.”
5. To validate that the control is working as intended, the security analyst must be engaged in the applicable joint application design sessions where the controls will be demonstrated. During the sessions, the security analyst will be able to validate that the implemented control is acting as intended. If the control cannot be implemented. The security analyst must work with the development team to create compensating controls (alternative forms of protection) to ensure that the spirit of the control is met.
6. It should be noted that there a base set of system-specific controls that must be implemented across the entire system. These include: Awareness and Training (AT), Auditing (AU), Assessment and Authorization (CA), Configuration Management (CM), Incident Response (IR), Maintenance (MA), Media Protection (MP), Planning (PL), Program Management (PM), Physical and Environmental (PE), and Risk Assessment (RA).
7. Finally, the development teams will need to ensure that the administrative controls have been addressed. These are implemented in the forms of policies that are issued by the governing agency.
2.1.1.3  System Security Plan Initialization

The SI Contractor security team will initiate the draft of the MMISR System Security Plan (SSP) in the planning phase. To perform this task, they will collaborate with the NM HSD security team and with their consent:

1. Require all MMISR component owners to use Volume IV: Affordable Care Act (ACA) Administering Entity System Security Plan (4 – MARS-E v2-0-AE-ACA-SSP-11102015.docx) template to develop a draft SSP for their respective modules. The template will be housed in the NM HSD security SharePoint site for accessibility.
2. The SI Contractor will then create a comprehensive MMISR SSP that will contain information on the Integration Platform in addition to the information from the draft SSPs created by the MMISR module contractors.
3. All module contractors will be required to update and review their SSPs drafts as needed and post their SSPs in the allocated location in the SharePoint site.
4. Module contractors are required to notify the NM HSD security team and the SI Contractor security team of any updates/changes to their SSP drafts via email. These updates must meet the requirements of the Architecture Review Board (ARB) for the SI Contractor team to incorporate them in the MMISR SSP.

2.1.2  Analysis

All module contractors including the SI Contractor will be required to conduct an Information System Risk Assessment (ISRA) of their individual modules, to determine all foreseeable security threats. Information security risk assessment is an on-going process of discovering, correcting, and preventing security problems. The risk assessment will help NM HSD determine the acceptable level of risk and the resulting security requirements for each system. The individual module contractors must then devise, implement, and monitor a set of security measures to address the level of identified risk.

The security risk assessment for new modules is conducted at the beginning of the SDLC. During the risk assessment of modules, the SI security team, and the module security team work in collaboration with relevant team members from the technical team, business team and information security officer to identify and assess the risks.

This risk assessment will be conducted annually and as needed thereafter. An additional need to conduct a risk assessment is in response to specific events such as when the system’s environment undergoes major modifications or in response to a security incident or audit.

This risk assessment methodology is based on the CMS Information Security Risk Assessment (RA) Methodology, developed by the Federal Department of Health and Human Services. The link provided to this document: CMS Risk Management Handbook (RMH)

The template used for the ISRA can be found on the link provided: ISRA template.

The SI Contractor security team will provide guidance and oversight to module contractors to develop or update their ISRAs as needed.

On completion, the ISRA artifact will:

• Summarize the system architecture and components of each MMISR module, and its overall level of security.
• Include a list of threat and vulnerabilities, the system’s current security controls, and its risk levels.
• Recommend safeguards to minimize the identified risks and describe the expected level of risk that would remain if these safeguards were put in place. The risk levels would be calculated using the NIST SP 800-30 risk calculation.
• Show where an organization needs to concentrate its remedial work.

Each of the module contractors will post their ISRAs in the NM HSD SharePoint security folder. On receiving the individual risk assessment of each MMISR module, the SI Contractor security team will work with the NM HSD security team to develop an integrated ISRA that will provide a comprehensive survey of risks and threats.

A Privacy Impact Analysis (PIA) will also be required during this phase. The PIA identifies the specific types of sensitive information that the each of the module contractors will collect, store, use, process, disclose, and/or disseminate.

To complete the PIA form, the module contractor must:

1. Obtain the latest PIA form from the SI Contractor and follow the instructions on the form.
2. Fill out all the sections in the template that are relevant for the module contractors.
3. On completing the PIA form, each module contractor must get it peer reviewed by the senior members of the security team and the SI Contractor security team.
4. A comprehensive MMISR PIA will be created by the SI Contractor by iteratively adding content from each of the module contractor’s PIAs. Each iteration will be reviewed and approved by NM HSD.
5. The PIA must be signed by the Chief Privacy Officer (CPO) and follow the CMS PIA approval process.
6. If a system undergoes a significant change at any time, the SI Contractor must be notified. The PIA will be updated with any changes that may impact the privacy safeguards of the system by the SI Contractor. NM HSD CPO must sign the updated PIA. Significant changes to an information system that may trigger the need for a security impact assessment (SIA) or an updated PIA include, but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications/configuration changes to system functionality, system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls.
7. Once the State CPO approves the PIA, he or she then sends it to the CMS Senior Agency Official of Privacy (SAOP) for final approval. The Senior Official of Privacy (SOP) reviews the completed CMS PIA and attests that it is adequately and accurately completed. The SOP then promotes/forwards the PIA to the Department and submits the completed CMS PIA to the SAOP or will seek revisions from the PIA author if errors are found.

The purpose of the PIA is to identify the risks and potential effects of collecting, maintaining, and disseminating PII. It also evaluates and documents the privacy safeguards to be followed to ensure that the confidentiality, integrity, and availability of the information is maintained.

2.1.3 Design

The objective of the design phase is to transform business requirements identified during previous phases into a detailed system architecture that is feasible, robust, and secure and brings value to the organization. The requirements identified in the requirements analysis phase are transformed into a system design document that accurately describes the design of the system and that can be used as an input to system development in the next phase.
The module contractor and the SI Contractor security teams will get involved from the initial stages of the design phase of their systems. Early involvement helps the developers and architects understand the security requirements from the initial stages. The security requirements for each system or module will be defined in collaboration with the SI Contractor. The SI Contractor and all module contractors will be required to submit a security design document. The SI security team, in collaboration with the NM HSD, will help module contractors identify vulnerabilities in their technology choices and help them follow specific requirements as outlined by the MARS-E v2.0 to overcome those vulnerabilities. By addressing these vulnerabilities in the design stage, the team can prevent those vulnerabilities from making it into the software and hardware during development.

NM HSD in collaboration with the SI Contractor, module contractors, and technical teams during the design phase will be done in the following manner:

- Schedule weekly or bi-weekly meetings to discuss the requirements of the MARS –E control families and the security requirements identified by the requirements team that are applicable to the design phase. Confirm that the technical team and developers are implementing all measures to be compliant with these controls. The SSP for each system will document the methodology and procedures for maintaining compliance with the controls.
- Maintain open communication via email and phone.
- Participate in Joint Application Development (JAD) sessions where security requirements are being demonstrated.
- Gain final approval of design from the architecture review board.
- Provide role-specific security training on threat modeling and architecture risk analysis, which will improve security during this phase of the SDLC.

### 2.1.4 Implementation

The purpose of the Implementation Phase is to deploy and enable operations of the MMISR system in the production environment.

For successful implementation of the MMISR system, the SI Contractor in conjunction with the module contractors and the NM HSD Security team will:

- Undergo a Security Control Assessment (SCA) of their systems. This assessment is conducted by a third-party assessor approved by NM HSD. (Please refer to 2.5 for more details on SCAs).
- Upon completion of the SCA, the SI Contractor will mitigate any findings discovered during the SCA. The SI Contractor will provide guidance to module contractor to mitigate the findings on their systems.
- On successful completion of the SCA, the SI Contractor in collaboration with the NM HSD security team will work on obtaining the Authority to Operate (ATO) for the MMISR system.

The outcome of the Implementation Phase is to deploy and enable operations of a secured MMISR system in the production environment and ensure its users are aware of their responsibility to protect the system.

### 2.1.5 Maintenance

The maintenance phase is the last stage of the SDLC. This phase occurs once the system is operational and involves making changes to hardware, software, and documentation to support its operational effectiveness. The outcome of the maintenance phase of the SDLC includes implementation of changes that software might undergo over a period or implementation of new requirements after the software is deployed at the customer location.
As systems and the environment in which they operate are dynamic, they need to be periodically reassessed by an independent assessor appointed by the State in the following manner:

- Conduct vulnerability assessment scans for the discovery and remediation of vulnerabilities periodically as specified (bi-weekly/weekly/monthly). These scans are conducted by the SI Contractor security engineers.
- Remediation of findings/vulnerabilities discovered by the scans should be conducted by each of the module contractors within 60 days of discovery. The SI Contractor will validate remediation.
- In the event there is a need for a critical security patch, the SI Contractor will develop policy that will entail holding an emergency CCB and gaining approval for implementation immediately.
- Conduct annual SCAs of the MARS-E v2.0 Security controls. (Please refer to Section 2.5 of this document). Some policies will differ depending on different systems and modules, as they will be unique in the type of data they store or process, their interconnecting systems, and their ability to maintain the required security posture. For example, systems that contain or process Federal Tax Information (FTI) will be required to meet the Internal Revenue Service (IRS) 1075 requirements.
- Provide artifacts or assist module contractors to provide artifacts for all security audits.
- Implement an incident response plan that addresses the coordination of events that will need to take place in the event of an incident or breach. All module contractors including the SI Contractor will be required to develop and implement an incident response plan for their respective systems.
- Conduct annual reviews and update of core security documentation.
- Conduct annual refresher security and privacy training for system users of the MMISR systems. NM HSD provides these mandatory online refresher courses.
- In coordination with the Change Control Board, the SI Contractor will assess any proposed change to determine the impact, if any, to the current security posture of the system. This is done by filling out a Security Impact Assessment (SIA) template that is available at the CMS security library.
- Create a corrective action plan using a Plan of Action and Milestones (POAM) document. This document will address the controls identified as ‘not satisfied’ or ‘partially satisfied’ during the SCAs. This document is housed on the NM HSD SharePoint site. The module contractors review these POAMs monthly until they can address the weakness and provide mitigation documents to support that the weakness has been addressed. If needed, the SI Contractor team will assist the module contractor in the creation of the POAM document and mitigation documents to address each weakness.

### 2.1.6 Applicable Standards

The following is a current list of applicable standards and regulations for the development of the Security Approach. This list is subject to change based upon new or revised standards.

- Federal Risk and Authorization Program (FedRAMP) certification in case any SI component or service is hosted in a Cloud environment.
- National Institute of Standards and Technology (NIST) Special Publication 800-131A, Revision 1.
• Federal Information Processing Standards (FIPS) 140-2, Security Requirements.
• Health Information Technology for Economic and Clinical Health (HITECH) Act.
• Health Insurance Portability and Accountability Act (HIPAA) of 1996.
• IRS Publication 1075.
• Center for Internet Security Benchmarks (https://www.cisecurity.org/cis-benchmarks/).
• New Mexico Administrative Code (NMAC) 1.12.20, Information Security Operation Management.
• Payment Card Industry (PCI) Data Security Standard (DSS).

The SI Contractor will share these standards and regulations with the security teams for the module contractors and help them understand and maintain compliance with the standards.

2.2 Minimum Acceptable Risk Standards for Exchanges

CMS has assembled a document suite of guidance, requirements, and templates known as the MARS-E v2.0. This suite of documents defines a risk-based Security and Privacy Framework for use in the design and implementation of the exchanges’ Information Technology (IT) systems, for which CMS has oversight responsibility.

The SI Contractor team will implement and maintain security controls, in collaboration with NM HSD and new module contractors, based on the MARS-E v2.0 security control set in the following manner

• Implement the Administrative controls by creating and or referencing the applicable policies in the SSP.
• Ensure that standard operating procedures and process are in place to address operation controls.
• Collaborate with the technical Subject Matter Experts (SMEs) in meetings and JAD sessions to ensure the technical safeguards are built in the Integrated Platform (IP).
• Establish operational procedures to ensure technical safeguards are maintained.

The SI contractor will also take into consideration other federal and State policies and standards. The SI Contractor will define these policies, procedures, and controls in the SSP.

This link below provides a description of the MARS-E v2.0 Security Family controls: MARS-E Security Control Descriptions.

This link is to the 4-MARS-E v2-0-AE-ACA-SSP template that will be used to create the SSP: 4-MARS-E v2-0-AE-ACA-SSP template.

2.3 PL-1 and PM-1 Controls

The PL-1 and PM-1 MARS-E v2.0 controls address the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the planning control family, which covers security-planning policies and procedures.
Policy and procedures reflect applicable federal and State laws, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organizational level may make the need for system-specific policies and procedures unnecessary. These policies can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The SI Contractor will establish the security planning procedures for the MMISR security. The organizational risk management strategy is a key factor in establishing policy and procedures.

According to the PL-1 control:

- The SI Contractor team develops, documents, and disseminates to applicable personnel a security planning policy that addresses scope, purpose, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- The SI Contractor team reviews and provides updates to procedures to facilitate the implementation of security planning policies and associated security-planning controls (as necessary) within every three hundred sixty-five-day period.

## 2.4 Security Artifacts

The security approach includes the delivery of security artifacts required by CMS, IRS Safeguard Computer Evaluation Matrix (SCSEM), HHS Office of the Inspector General (OIG), SSA, etc., for the security controls assessments and NM HSD. These security artifacts are system specific security documents that the SI Contractor security team and the module contractor security teams develop and deliver. The SI Contractor is responsible for developing artifacts for their own systems and then for soliciting, obtaining, and reviewing the artifacts of the other module contractors.

The NM HSD security team approves these artifacts, after which CMS reviews and approves the artifacts. These artifacts are used during the Security Control Assessment of each system/module. The list of artifacts below is outlined below:

- **System Security Plan:** The SSP will be the primary source for the descriptions of the implementation, methodology, and compliance status of each control outlined in the CMS-approved MARS-E v2.0. The SSP provides a high-level description of the decisions made regarding the definition of system boundaries of the systems in consideration, as well as any system interconnections and dependencies. It also identifies the relationships between existing systems (both internal and external) and the potential relationships between new systems and modules.
  - Part A of the SSP provides a summary description of each MMISR component/system and associated security architecture and components.
  - Part B will contain the security and privacy controls that are in place to protect the SI platform.
  - Part C refers to the privacy controls listed under Part B.
  - Part D will contain IRS requirements for safeguarding FTI.
  - Part E will contain attachments to support the information provided in Parts A and B.
- **Security Design Plan:** This document details the security design of the security components for the SI platform. This includes the technical architecture for security-related components in the SI platform, including the Identity and Access Management (IdAM) environment, the Splunk Security Information Event Management (SIEM) solution, and the Oracle API Manager, IdAM.
and Service Oriented Architecture (SOA) Gateway. This document will contain logical and physical architectural depictions of security, as well as integration points with the SI platform.

- **Privacy Impact Analysis (PIA):** This document identifies the specific types of sensitive information that the contractor will collect, store, use, process, disclose, and/or disseminate. It also documents how the administering entity analyzes the privacy risks associated with maintaining that information, and how the SI Contractor subsequently documents this analysis. The document contains privacy and security standards for its business partners and other third parties. It will also contain the agreements that bind these entities, and outline incident handling procedures, and privacy and/or security awareness programs. The document outlines the legal environment (legal authorities and State privacy laws) that will need to be addressed for privacy of data.

- **Information System Risk Assessment (ISRA):** This document provides structured identification of risk exposure for the SI Platform. It addresses threats, vulnerabilities, and risks, as well as recommending appropriate safeguards (security controls) in support of continued business operations.

- **Security Certification and Accreditation Letters:** In these letters, the SI Contractor and MMISR Contractors provide the content required to obtain certification and accreditation letters from CMS. The information provided in the letters summarize the security posture of the individual system and indicate that the required security and privacy artifacts have been completed to obtain the ATO.

- **Security Questionnaire Document:** The Security Questionnaire Document will include the questions required to assess the readiness of the MMISR module contractors to meet IP standards. Questionnaires will include questions to evaluate the MMISR module contractors in the following categories:
  - Security and privacy policy, procedures, and standards
  - IdAM
  - Security auditing, logging, and reporting
  - Data encryption
  - System boundary protection and infrastructure security
  - Applicable management, operations, and technical controls from the SSP

The security questionnaire will also inquire as to whether a contractor’s SI solution meets each security requirement out-of-the-box, whether it will meet it, but customization is required, or if a requirement cannot be met.

The module contractors will develop and deliver these core documents to the client within an agreed upon timeline. The SI Contractor team will review these documents for accuracy.

### 2.5 Security Control Assessments

Security Control Assessments (SCAs) are conducted to evaluate the security controls for a system over a period of three years. A full assessment is conducted every four-years, while one-third of the controls (which includes a required base set of controls) are assessed annually. These controls are defined in the MARS-E v2.0 security framework. The IP and all participating systems and modules undergo a SCA by a third-party assessor (SCA Team) per the MARS-E v2.0 CA-2 control. NM HSD will select the third-party assessor.

Each MMISR component including the SI Platform must undergo a SCA that includes:
• An assessment by a third-party assessor to determine if the selected set of controls have been implemented correctly and are working as intended (Please refer to Section 2.5 of this document).
• Coordination with the SCA team so that stakeholders, system components, policies, etc., are available for interviewing, testing, and reviewing, as appropriate.
• A Risk Assessment Report (RAR) with the SCA team findings, to be provided to NM HSD, the module contractors, and the SI Contractor.
• Subsequent mitigation activities between the SI team and the module contractors as necessary to resolve weakness and findings identified in the RAR to obtain and/or maintain an ATO.

The NM HSD security team will provide the guidelines to obtain the ATO for the MMISR. These guidelines will be posted on the NM HSD SharePoint Site. As each module completes the security controls assessment with an acceptable level of risk (as determined by the CMS authorizing official), that module will be added to the overall MMISR authorization boundary. If an acceptable level of risk is not obtained, the SI Contractor will work with the module contractor to remediate weaknesses (updating policies, updating SSP, obtaining additional artifacts, etc.) until an acceptable level of risk is achieved. The SI Contractor, module contractors, and the NM HSD security team will keep an open communication to clarify any questions or doubts, via email and conference calls.

Coordination of the module contractors and the SI Contractor with the security controls assessment teams during an SCA include the following steps:

• Provide all documents and information the assessment team needs to conduct the SCA.
• Schedule weekly or monthly meetings to provide updates and discuss any issues.
• Maintain open communication via email, meetings and phone conferences.

The SI Contractor security team will participate in the SCAs as needed. They will:

• Orchestrate interviews and provide artifacts needed for the SI SCA.
• Review and provide feedback for the documents and artifacts that need to be submitted by the module contractors for the SCA.
• Assist the module contractors on mitigating any SCA findings if needed. The CA-2 control of the Security Assessment and Authorization Control family of MARS-E v2.0 provides details on SCAs.

2.6 Security Activities

The SI Contractor will take all necessary steps to follow and share with module contractors required security activities. The SI Contractor will participate in Security Governance processes as needed.

2.6.1 Personnel Screening

The security teams for the module contractors will work with their respective Human Resource (HR) departments to follow a secure Personnel Screening (PS) process in compliance with the MARS-E v2.0 PS-3 control and NM HSD policies.

As part of the on-boarding process, the SI Contractor currently conducts background checks for its own employees. The SI Contractor team will also perform project-specific background checks to be consistent with NM HSD and federal and State policies and requirements for staff security prior to authorizing access to any information systems. All module contractors across the HHS 2020
environment will be required to conduct their own PS process as outlined in the PS-3 in the MARS-E v2.0 suite of security controls.

2.6.2 SI Project Personnel Security

In compliance with NM HSD personnel security requirements, the SI Contractor security team will:

- Require the SI Contractor and module contractor staff to comply with NM HSD and MARS-E v2.0 personnel security policies and procedures.
- Ensure all SI Contractor and module contractor staff complete NM HSD-provided online security-related training when they join the project and undergo training at least annually for:
  - Security Awareness
  - IRS Safeguards
  - HIPAA Training
  - Privacy Training (for information system users)
- Obtain signed or electronic (e.g., Learning Management System acknowledgment) individual security training acknowledgments for each contractor or subcontractor, and provide these to the NM HSD CISO for initial training and for annual re-certifications.
- Monitor staff compliance with these security requirements by using a Training Tracking Log that would be located in the NM HSD SharePoint site.
- Ensure those module contractors requiring access to the NM HSD SharePoint portal complete the Security Access Request (SAR) form and submit it to the NM HSD Information Technology Department (ITD) Help Desk. Once approval from the NM HSD security team has been obtained, the System Administrator provides access to the user based on their role and privileges.
- Notify NM HSD within one (1) business day of any personnel transfers or termination of SI team or subcontractor personnel who have NM HSD credentials or badges, or who have information system privileges per MARS-E PS-4 and PS-5 controls. All module contractors across the HHS 2020 environment are required to conduct the personnel transfer and termination process as outlined in the Personnel Screening controls PS-5 and PS-4 described in the MARS-E v2.0 security controls.

2.6.3 Termination

Upon termination of an individual’s employment or participation in the MMISR project, and consistent with NM HSD policies and procedures, the SI Contractor and module contractor teams will:

- Disable information system access for that individual immediately or as soon possible. Accounts will be configured to “disabled” within the Windows Active Directory such that all active accounts under the specific user will no longer be active and accessible to the system.
- Terminate or revoke any authenticators or credentials associated with the individual.
- Submit the applicable “Delete All Security Access Request” forms to the NM HSD ITD Help Desk.
- Retrieve all security-related NM HSD property.
- Assume control of access to NM HSD information or information systems formerly controlled by the terminated individual.
- Notify the NM HSD CISO upon termination of the employee.
- Prohibit physical access to NM HSD and to contractor facilities (e.g., disable badges, change access codes).
2.6.4 Rules of Behavior

Prior to accessing the NM HSD computer network, the SI Contractor security team and module contractor staff must read the NM HSD Use of State Information Technology Resources policy, and sign and return it to the NM HSD CISO. They must also sign and return the NM HSD Information Technology Resource Usage policy that commits them to comply with NM HSD policy. Additionally, they are required to follow the rules of behavior (PL-4) as outlined in MARS-E v2.0 security framework.

2.6.5 Physical Access to Facilities and Computers

SI Contractor and module contractor staff who have access to State or MMISR Contractor facilities or computers where confidential information resides will follow the tasks listed below to secure their individual facilities that are maintained by the SI Contractor or the module contractors. The team will also refer to the Physical and Environment Protection (PEP) family control outlined in the MARS-E v2.0 security framework:

- Develop, approve, and maintain a list of SI Contractors, and module contractors with authorized access. This list will reside on the NM HSD SharePoint site.
- Issue and manage authorization credentials for facility access as appropriate.
- Remove individuals from the facility access list within one (1) business day when access is no longer required.
- Ensure control of SI Contractor and module contractor facility ingress and egress by requiring access control systems or guards, as well as verification of access authorization before granting access to a facility.
- Maintain a physical access audit log for visitors to facilities, including at a minimum the name of the person, as well as the date and time of access.
- Ensure that visitors to the SI Contractor and module contractor facilities are escorted and monitored.
- Secure keys, combinations, or other physical access devices associated with SI Contractor and module contractor facility(s).
- Maintain an inventory of physical access devices.
- Change facility lock combinations annually or whenever an employee who knows the combination is retired, terminated, or transferred to another position.
- Change keys when a master key has been lost.
- Ensure that all computers meet NM HSD security requirements by validating baselines against MARS-E v2.0 and NM HSD requirements using vulnerability and configuration scans.

2.6.6 Remote Access

Remote access is any access to an information system by a user who is communicating through an external network (e.g., the internet). Any remote access to NM HSD confidential information is required to be performed using multi-factor authentication and Virtual Private Network employing FIPS 140-2 approved encryption. The SI Contractor will adhere to NM HSD usage restrictions, configuration, and connection requirements and implementation guidance for each type of remote access granted. The System/Network Administrator will maintain a list of users that have remote access to confidential information and provide role-based access to users. The Information System Security Officer (ISSO) approval is required for remote access for valid business reasons, or as needed.
2.6.7 Confidential Information

The SI Contractor, module contractor, employees, agents, representatives, or other staff located offshore (i.e., outside of the United States and its territories, embassies, or military installations) will not be granted access to confidential information via remote access.

2.6.8 Use of External Information Systems

Unless approved by the NM HSD CISO, the SI Contractor will prohibit:

- Access to confidential information from external information systems.
- Use of non-NM HSD-owned information systems, system components, or devices to process, store, or transmit confidential information.

To adhere to the federal policies and procedures regarding the use of external information systems, the SI team refers to the AC-20 family control from the MARS-E v2.0 security control framework.

2.6.9 Media

To adhere to the federal policies and procedures regarding Media Protection (MP), the SI Contractor refers to the MP family control from the MARS-E v2.0 security control framework.

2.6.10 Email Communications

The SI Contractor will adhere to NM HSD policies and procedures regarding inclusion of FTI, Protected Health Information (PHI), Personally Identifiable Information (PII), or other sensitive, confidential, or private data within email communications. The NM HSD SharePoint site will house these policies and procedures.

- The SI Contractor team will encrypt emails with sensitive information by using tools defined in the policies outlined by NM HSD to provide end-to-end security and compliance. For example, utilize public key encryption for emails containing sensitive information.

3. Team Members

The SI Contractor and module contractors will be required to provide a list of their team members as described in the subsections below. This information will be contained in the SSP.

3.1 Certification and Accreditation Team

Each interacting system/module will be required to fill out the information provided below in their individual System Security Plans (SSPs), if applicable, as noted in Table 1.

<table>
<thead>
<tr>
<th>Project Role</th>
<th>NM HSD</th>
<th>SI Contractor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Information Officer</td>
<td>Sean Pearson</td>
<td>Henry Hutson</td>
</tr>
<tr>
<td>Chief Information Security Officer</td>
<td>Sean Pearson</td>
<td>Tonya Love</td>
</tr>
</tbody>
</table>
3.2 Security Team

All module and system contractors are required to provide the following role descriptions in their individual SSPs. Table 2 provides a description of the roles and responsibilities of the security team. The module and system contractors will identify the roles that are applicable within their organization.

Table 2: Security Team Roles and Responsibilities

<table>
<thead>
<tr>
<th>Roles</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Owner (BO)</td>
<td>The Business Owner:</td>
</tr>
<tr>
<td></td>
<td>• Responsible for conducting organizational mission/business functions</td>
</tr>
<tr>
<td>Chief Information Officer (CIO)</td>
<td>The CIO:</td>
</tr>
<tr>
<td></td>
<td>• Defines mandatory information security and privacy training, education, and awareness activities undertaken by all personnel, including contractors.</td>
</tr>
<tr>
<td></td>
<td>• Creates and manages the review and approval of changes through the appropriate change control bodies/boards.</td>
</tr>
<tr>
<td>Chief Privacy Officer (CPO)</td>
<td>The CPO, or other designated official responsible for privacy compliance across an organization including privacy compliance measures that apply to information security assets and activities:</td>
</tr>
<tr>
<td></td>
<td>• Maintains a balance between security and privacy requirements and ensures that one is not compromised for the sake of the other.</td>
</tr>
<tr>
<td></td>
<td>• Is responsible for developing, promoting, and supporting the organization’s privacy programs.</td>
</tr>
<tr>
<td></td>
<td>• Encourages awareness of potential privacy issues and policies.</td>
</tr>
<tr>
<td></td>
<td>• Reviews and implements privacy regulations and legislation.</td>
</tr>
<tr>
<td>Information System Owner (ISO)/System owner</td>
<td>The ISO is the agency official responsible for the overall procurement, development, integration, modification, and operation and maintenance of the information system.</td>
</tr>
</tbody>
</table>
## Roles and Responsibilities

<table>
<thead>
<tr>
<th>Roles</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| Chief Information Security Officer (CISO)    | The CISO:  
• Defines information security and privacy control requirements.  
• Delegates the authority to approve system configuration deviations to the CRA and ISSO, where appropriate.  
• Ensures CMS-wide implementation of HHS and CMS information security and privacy capabilities, policies, and procedures.  
• Can also serve as the Senior Information Security Officer. |
| Information System Security Officer (ISSO)   | The ISSO is the agency official assigned responsibility by the SAISO, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program. |

The following sites provide a detailed description of these roles, as defined by CMS:

- CMS Policy for Information Security and Privacy – Roles and Responsibilities
- NIST Special publication 800-100-Roles and Responsibilities

The information for each role can be contained in a Role Matrix as shown in the Table 3.

### Table 3: Role Matrix

<table>
<thead>
<tr>
<th>Name</th>
<th>Business Owner</th>
<th>CIO</th>
<th>Information System Owner</th>
<th>CISO</th>
<th>ISSO</th>
<th>Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Name&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;Title&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;Organization&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;Email&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;Phone&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The module contractors will house the above information in their individual SSPs.

## 4. System Categorization

### 4.1 MMISR Modules

The Business Process Outsourcing (BPO) systems and the IP are part of the MMISR solution and are identified as MMISR modules. A list of these MMISR modules follows:

- System Integrator
- Benefits Management Services (BMS)
• Data Services (DS)
• Financial Service Module (FSM)
• Quality Assurance (QA)
• Unified Public Interface (UPI)

The MMISR module contractors are required to fill out the information provided in the table in Appendix D of this document. This information will be contained in the SSP for each individual system. The module contractors may need to provide additional information as needed.

4.2 Integration Platform Components

The Integration Platform (IP) is composed of components. A component is capable of fulfilling specific functionalities of the system. The IP will integrate the following modules:

• Integrated Platform
• System Migration Repository (SMR)
• Master Data Management (MDM)
• Enterprise Service Bus (ESB)
• Identity and Access Management (IdAM)
• Electronic Document Management (EDM)
• Client Communication Management (CCM)
• Address Standardization (AS)

Module contractors are required to fill out the information provided in Appendix D of this document. This information will be contained in the SSP of each system, along with all technical and boundary diagrams. The component owner may need to provide additional information as needed. The MMISR SSP will consolidate the information from the individual SSPs.

4.3 Interconnected Systems

Interconnected systems are the systems that the MMISR module communicates with to fulfill specific business functionalities. The MMISR SSP will identify each interconnected system and ensure that relevant security controls are implemented in compliance with MARS-E control sets. The interconnected systems are expected to provide approved Data Use Agreements (DUA), Memorandum of Understanding (MOU) or Information Security Agreements (ISA) to NM HSD to ensure privacy and confidentiality of the data.

5. Programmatic Activities

Programmatic activities include areas such as team training, configuration management, risk management, and communication plans. These activities support the overall security approach.

5.1 Team Training

All module contractors are made aware of the security and other standards (e.g., transmission, database, data at rest) that are established for the MMISR system. The new module and system contractors will be directed to read Governance Standards – Technical and Architectural. This document provides the governance and standards for the MMISR project and is located on the NM HSD SharePoint site.
Security training will be provided to all onboarding members of the MMISR project and module contractors and will be located in the NM HSD SharePoint site. These trainings will be provided by the SI Contractor and NM HSD. The onboarded members will be directed to read The Staffing Model and Resource Management Plan. This document provides detailed description of the onboarding and off-boarding activities. This document is located on the NM HSD SharePoint site.

All users will be required to take online trainings provided by NM HSD. It is mandatory to take these trainings on an annual basis. NM HSD automatically keeps a record of the trainings taken by the employees and system and module contractors.

The SI Contractor will also provide online trainings via available web tools. An example of these trainings would be role based training for developers and testers.

The module and system contractors will receive training from the SI Contractor to prepare for the SCAs.

The SI Contractor will review the documentation prepared by the module contractors and provide feedback. This will be done via conference calls, WebEx and email.

The SI Contractor security team will maintain a security training tracker for this purpose. This training tracker will be housed in the NM HSD SharePoint site. The SI Contractor will follow all the training guidance outlined by NM HSD.

Each module contractor including the SI Contractor will be expected to provide role-specific security training.

5.2 Configuration Management

All module contractors will be directed to the Configuration Management Plan (CMP) that is located on the NM HSD SharePoint site. The document can be found at the following NM HSD SharePoint site: Configuration Management Plan.

The CMP is an enterprise document that will contain the configuration requirements that the MMISR components are required to abide by. This is done to ensure that changes to the system are carefully managed and thought out.

The module and system contractors will use the configuration list to design and develop their systems. They will collaborate with the SI Contractor to verify the accuracy and efficiency of the configuration items they choose. This collaboration will be done via email, conference calls and WebEx.

The SI Contractor will provide training on the Configuration Management Database Tools (CMDB) to NM HSD. This training will be provided via available web tools. Training materials will be provided by the SI Contractor.

5.3 Risk Management

All module contractors will be directed to the Risk Management Plan (RMP) that is located on the NM HSD SharePoint site. The RMP is an enterprise document that is intended for use by project executive oversight and State and federal partners to gain a clear yet succinct understanding of the project risk management practices. Risk management is important as tracking program vulnerabilities can have a direct impact on the security program’s ability to track, mitigate and monitor vulnerabilities for the MMISR system.
All security risks will be identified by and of the HHS 2020 enterprise stakeholders and will be logged in the risk register in accordance with the RMP. All risks will be reviewed on a weekly basis with NM HSD as described in the RMP.

The RMP for the SI platform can be found on the NM HSD SharePoint site:

- Risk Management
- Risk Register

5.4 Change Management

All module contractors will be directed to the Change Control Management Plan (CCMP) that is located on the NM HSD SharePoint site. The document can be found at the following NM HSD SharePoint site: Change Control Management Plan.

All security related change requests are required to follow the protocol outlined in the CCMP. This will ensure that standardized methods and procedures are used for efficient and prompt handling of all change request. It will help to ensure that changes are authorized and thoroughly considered (i.e. PIA) to minimize security impacts to the MMISR Project.

6. CMS Certification

This section will document the approach to MMIS Certification in relation to the Security Approach. Appendix E of the Medicaid Enterprise Certification Toolkit (MECT) identifies the Security Approach as integral to the design of the database as part of the technical component of SDLC. The Centers for Medicare and Medicaid Services (CMS) formally reviews the Security Approach during the Medicaid Enterprise Certification Life Cycle (MECL) while conducting the following reviews:

- R2, Operational Milestone Review
- R3, MMIS Certification Final Review

This deliverable may also be reviewed during informal CMS reviews, including consults and gate reviews.

Appendix E: MECT Checklist contains the items that are attributable to the Security Approach.

7. Assumptions, Constraints, and Risks

This section documents assumptions, constraints, and risks for the deliverable.

7.1 Assumptions

The following assumptions have been identified, which may be updated over time:

- MMISR resources are available to participate in Security Approach implementation.
- MMISR module contractors will support the Security Approach.
- The NM HSD Data Center complies with the New Mexico State Policies and Standards in addition to MARS-E v2.0.
7.2 Constraints

No constraints have been identified at this time.

7.3 Risks

The following risks have been identified, which may be updated over time:

- If certain legacy systems are not technologically compliant with the MMISR security requirements, this may require additional development of security functions for integration with the MMISR systems.
- As the Oracle Cloud environment is not yet FedRAMP-certified, the system may not receive its ATO. If it does not receive an ATO, it will not be allowed to deploy.
- The module and systems will be developed only after the module or system contractors are awarded the contract. This would result in delays in completing the core security documents like the SSP in time for the security controls assessment.

All project risks will be updated and managed according to the Risk Management Plan.

8. Requirements Traceability

This section documents requirements satisfied by the deliverable, in the following form.

This deliverable meets the following requirements:

- Request for Proposal (RFP): Page 111. Section 2.2.1.12
- Proposal: Page 59. Section 1.3.4.1.1.11
- Statement of Work (SOW): Security1
- NM HSD Decision Log Entry #31: Configuration and Continuous Integration Services (CCIS)
- Deliverable Scope Change
9. Appendices

9.1 Appendix A: Record of Changes

Table 4 provides the deliverable record of changes.

**Table 4: Deliverable Record of Changes**

<table>
<thead>
<tr>
<th>Version Number</th>
<th>Date</th>
<th>Author/Owner</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>v0.1</td>
<td>08/24/18</td>
<td>Hans Bhatia</td>
<td>Initial Draft Created</td>
</tr>
<tr>
<td>v0.2</td>
<td>09/07/2018</td>
<td>Sangeeta Sinha</td>
<td>Review and update</td>
</tr>
<tr>
<td>V1.0</td>
<td>09/21/2018</td>
<td>SI Contractor</td>
<td>Final</td>
</tr>
<tr>
<td>v.03</td>
<td>10/17/2018</td>
<td>Sangeeta Sinha</td>
<td>Made changes as per the collaboration meeting</td>
</tr>
<tr>
<td>v.04</td>
<td>11/5/2018 through 11/26/18</td>
<td>SI Contractor Security team</td>
<td>Made changes as per the comments made on 11/5/2018 and added RACI chart</td>
</tr>
<tr>
<td>v.05</td>
<td>11/26/18-1/18/19</td>
<td>SI Contractor Security team</td>
<td>Made changes per collaboration meetings</td>
</tr>
<tr>
<td>V1.0</td>
<td>2/1/19</td>
<td>SI Contractor</td>
<td>Final Version published</td>
</tr>
</tbody>
</table>

9.2 Appendix B: List of Acronyms

Table 5 provides a list of project-specific acronyms used in this document. For a comprehensive, project-wide list of acronyms, consult the Master Acronyms list on the SI Contractor team SharePoint site at Shared Resources on SharePoint.

**Table 5: List of Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACA</td>
<td>Patient Protection and Affordable Care Act of 2010, or Affordable Care Act</td>
</tr>
<tr>
<td>AS</td>
<td>Address Standardization</td>
</tr>
<tr>
<td>ATO</td>
<td>Authority to Operate</td>
</tr>
<tr>
<td>BMS</td>
<td>Benefit Management Services</td>
</tr>
<tr>
<td>BPO</td>
<td>Business Process Outsourcing</td>
</tr>
<tr>
<td>BO</td>
<td>Business Owner</td>
</tr>
<tr>
<td>C&amp;A</td>
<td>Certification and Accreditation</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>CCMP</td>
<td>Change Control Management Plan</td>
</tr>
<tr>
<td>CISO</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td>CCM</td>
<td>Client Communication Management</td>
</tr>
<tr>
<td>CMDB</td>
<td>Configuration Management Database Tools</td>
</tr>
<tr>
<td>CMP</td>
<td>Configuration Management Plan</td>
</tr>
<tr>
<td>CMS</td>
<td>Centers for Medicare and Medicaid Services</td>
</tr>
<tr>
<td>CPO</td>
<td>Chief Privacy Officer</td>
</tr>
<tr>
<td>DS</td>
<td>Data Services</td>
</tr>
<tr>
<td>DSS</td>
<td>Data Security Standard</td>
</tr>
<tr>
<td>EDM</td>
<td>Electronic Document Management</td>
</tr>
<tr>
<td>ePhI</td>
<td>Electronic Protected Health Information</td>
</tr>
<tr>
<td>ESB</td>
<td>Enterprise Service Bus</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>Federal Risk and Authorization Management Program</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Management Act</td>
</tr>
<tr>
<td>FPLS</td>
<td>Federal Parent Locator Service</td>
</tr>
<tr>
<td>FSM</td>
<td>Financial Service Module</td>
</tr>
<tr>
<td>FTI</td>
<td>Federal Tax Information</td>
</tr>
<tr>
<td>GSS</td>
<td>General Support System</td>
</tr>
<tr>
<td>HHS</td>
<td>Health and Human Services</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HITECH</td>
<td>Health Information Technology for Economic and Clinical Health Act</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resource</td>
</tr>
<tr>
<td>HSD</td>
<td>Human Services Department</td>
</tr>
<tr>
<td>IdAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>IP</td>
<td>Integration Platform</td>
</tr>
<tr>
<td>IRS</td>
<td>Internal Revenue Service</td>
</tr>
<tr>
<td>ISA</td>
<td>Information Security Agreement</td>
</tr>
<tr>
<td>ISO</td>
<td>Information System Owner</td>
</tr>
<tr>
<td>ISRA</td>
<td>Information System Risk Assessment</td>
</tr>
<tr>
<td>ISSO</td>
<td>Information System Security Officer</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITD</td>
<td>Information Technology Department</td>
</tr>
<tr>
<td>JAD</td>
<td>Joint Application Development</td>
</tr>
<tr>
<td>MA</td>
<td>Major Application</td>
</tr>
<tr>
<td>MARS-E</td>
<td>Minimum Acceptable Risk Standards for Exchanges</td>
</tr>
<tr>
<td>MECT</td>
<td>Medicaid Enterprise Certification Toolkit (MECT)</td>
</tr>
<tr>
<td>MDM</td>
<td>Master Data Management</td>
</tr>
<tr>
<td>MMISR</td>
<td>Medicaid Management Information System Replacement</td>
</tr>
<tr>
<td>MP</td>
<td>Media Protection</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NM</td>
<td>New Mexico</td>
</tr>
<tr>
<td>NMAC</td>
<td>New Mexico Administrative Code</td>
</tr>
<tr>
<td>OIG</td>
<td>Office of the Inspector General</td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry</td>
</tr>
<tr>
<td>PEP</td>
<td>Physical and Environment Protection</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Analysis</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PL-1</td>
<td>Planning-1</td>
</tr>
<tr>
<td>PM-1</td>
<td>Program Management-1</td>
</tr>
<tr>
<td>POAM</td>
<td>Plan of Action and Milestones</td>
</tr>
<tr>
<td>PS</td>
<td>Personnel Screening</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>RAR</td>
<td>Risk Assessment Report</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Proposal</td>
</tr>
<tr>
<td>SAOP</td>
<td>Senior Agency Official for Privacy</td>
</tr>
<tr>
<td>SAR</td>
<td>Security Access Report</td>
</tr>
<tr>
<td>SCA</td>
<td>Security Controls Assessment</td>
</tr>
<tr>
<td>SCSEM</td>
<td>Safeguard Computer Security Evaluation Matrix</td>
</tr>
<tr>
<td>SOW</td>
<td>Statement of Work</td>
</tr>
<tr>
<td>SDLC</td>
<td>System Development Life Cycle</td>
</tr>
</tbody>
</table>
### Appendix C: Glossary

Table 6 is a glossary of project-specific terminology will be maintained on the SI Contractor team SharePoint site.

#### Table 6: Glossary

<table>
<thead>
<tr>
<th>Item Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Rule</td>
<td>A business rule is a statement that describes a business policy, procedure, guideline, standard, or regulation upon which the business operates.</td>
</tr>
<tr>
<td>HHS 2020</td>
<td>The vision for an ecosystem of HHS-related departments and supporting systems working cooperatively to improve outcomes for citizens while reducing operational costs for the State and increasing the use of shared data.</td>
</tr>
<tr>
<td>MMISR</td>
<td>MMISR Systems/Services contains all outsourced systems, solutions, modules, applications, and/or services licensed/implemented through the distinct procurements.</td>
</tr>
<tr>
<td>System</td>
<td>System is representation of software or a hardware unit which performs a set of business processes enters for CMS.</td>
</tr>
<tr>
<td>Single Sign-On</td>
<td>Single Sign-On (SSO) is an authentication process that allows a user to access multiple applications with one set of login credentials.</td>
</tr>
</tbody>
</table>
## 9.4 Appendix D: MMISR Modules and Components Information

Table 7 provides MMISR modules and components information.

### Table 7: MMISR Modules and Components Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description/Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>&lt;Name of the system&gt;</td>
</tr>
<tr>
<td>System Description</td>
<td>&lt;Purpose of the system&gt;</td>
</tr>
<tr>
<td>Security Manager</td>
<td>&lt;Identify the security manager for this system&gt;</td>
</tr>
</tbody>
</table>
| Characterization | The system is characterized as a <General Support System (GSS), Major Application (MA) or Other>.  
  - A “general support system" or "system" means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).  
  - A "major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight. Adequate security for other applications should be provided by security of the systems in which they operate. |
| Categorization   | FIPS 199 requires Federal agencies to assess their information systems in each of the categories of confidentiality, integrity and availability, rating each system as low, moderate, or high impact in each category. The most severe rating from any category becomes the information system’s overall security categorization. For the purposes of the MMISR all modules will be categorized as Moderate. |
| Data Classification | Data classification is the process of organizing data into categories for its most effective and efficient use. The purpose of this step is to help broadly identify the HHS 2020 enterprise datasets, along with their sensitivity, |


criticality, and characterization for each of the HHS 2020 enterprise datasets. It is a multi-step process that includes:

- Classifying HHS 2020 Data into groups: ePHI, PHI, PII, PCI, FTI, or Federal Parent Locator Service (FPLS).
- Characterizing the data as Public, Internal, or Confidential.

<table>
<thead>
<tr>
<th><strong>Boundaries</strong></th>
<th>This section will include a high-level description of the security services or components that will be included in the part of the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dependencies</strong></td>
<td>This section will include a description of the security services or components that are inherited from a system with a characterization of General Support System (GSS) or Major Application (MA).</td>
</tr>
<tr>
<td><strong>Interconnections</strong></td>
<td>A description of other system interconnections established for data sharing, business continuity, or backup.</td>
</tr>
</tbody>
</table>
9.5 Appendix E: RACI CHART

The RACI Chart is a Responsible, Accountable, Consulted, Informed (RACI) chart that assigns roles to activities. Below is the key to the symbols used in Tables 9 and 10:

- **R** = Responsible (doer) – Individual(s) performing the action/task. It means doing the “work.”
- **A** = Accountable (owner) – The individual(s) responsible for the decision and directing the individual(s) responsible for the task. The individual(s) held accountable that the action/task is completed.
- **C** = Consulted (resource) – The individual(s) having deep insight and providing consultancy.
- **I** = Informed (FYI) – The individual(s) needing to know the decisions made or actions taken.

Table 8 MMISR Roles and Responsibilities RACI Chart

<table>
<thead>
<tr>
<th>Action/Task</th>
<th>NM HSD MMISR Security Team</th>
<th>TPGSI Security Team</th>
<th>SI Technical Team Members</th>
<th>SI Business Analyst</th>
<th>SI Developers /Testers</th>
<th>NM HSD Privacy Officer</th>
<th>TPGSI QA Team</th>
<th>IV&amp;V Team</th>
<th>NM HSD</th>
<th>Architecture Review Board (ARB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Planning (Security Deliverables)</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td>C</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Requirements Analysis</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Design</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Security Testing</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Training</td>
<td>I</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>Action /Task</td>
<td>NM HSD MMISR Security Team</td>
<td>TPGSI Security Team</td>
<td>BPO Contractor Technical/Security Team Members</td>
<td>BPO Contractor Business Analyst</td>
<td>BPO Contractor Developers/Testers</td>
<td>NM HSD Privacy Officer</td>
<td>TPGSI/BPO QA Team</td>
<td>IV&amp;V Team</td>
<td>NM HSD</td>
<td>Architecture Review Board (ARB)/BPO</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------</td>
<td>--------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------</td>
<td>------------------</td>
<td>-----------</td>
<td>-------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Security Planning (Security Deliverables)</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td></td>
<td>C</td>
<td>R</td>
<td>R</td>
<td>I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Requirements Review</td>
<td>A</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 9: Business Process Outsourcing Contractor Specific
<table>
<thead>
<tr>
<th>Action /Task</th>
<th>NM HSD MMISR Security Team</th>
<th>TPGSI Security Team</th>
<th>BPO Contractor Technical/Security Team Members</th>
<th>BPO Contractor Business Analyst</th>
<th>BPO Contractor Developer/Testers</th>
<th>NM HSD Privacy Officer</th>
<th>TPGSI/BPO QA Team</th>
<th>IV&amp;V Team</th>
<th>NM HSD</th>
<th>Architecture Review Board (ARB) /BPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Design Review</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Security Testing Review</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Training</td>
<td>A</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
</tr>
<tr>
<td>SCSEMS (Vulnerability testing, IRS 1075 scans etc.)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Patching Planning</td>
<td>A</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>I</td>
</tr>
<tr>
<td>Software Patching</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>