Medicaid Management Information System Replacement (MMISR) Project

SECURITY3: Security Design Plan

NM HSD Deliverable Owner: Sean Pearson
Contractor Deliverable Owner: Tonya Love
Configuration Number v1.0
April 5, 2019

TurningPoint
Turning Point Global Solutions
Software Services Company™
# Table of Contents

1 Introduction .......................................................................................................................... 1  
   1.1 Overview........................................................................................................................ 1  
   1.2 Audience....................................................................................................................... 1  
   1.3 Purpose.......................................................................................................................... 1  
2 Security Design Overview..................................................................................................... 2  
   2.1 System Security Description.......................................................................................... 2  
   2.2 Security Architecture.................................................................................................... 2  
      2.2.1 Infrastructure/Network............................................................................................ 2  
      2.2.2 Operating System/Network................................................................................... 3  
      2.2.3 Platform ................................................................................................................ 3  
      2.2.4 Enterprise Shared Services.................................................................................... 4  
      2.2.5 Disaster Recovery.................................................................................................. 5  
   2.3 Applicable Standards........................................................................................................ 5  
3 Security of Physical Premises ............................................................................................... 6  
4 Identification, Authentication, and Authorization................................................................. 7  
   4.1 Identification and Authentication.................................................................................... 7  
      4.1.1 Web Services Authentication................................................................................. 7  
      4.1.2 UPI Portal Authentication...................................................................................... 7  
   4.2 Access Management and Non-Privileged HSD User Data .................................................. 9  
      4.2.1 Server Authentication – Web Services................................................................. 10  
      4.2.2 User Authentication – Web Services.................................................................... 10  
5 Logging and Auditing............................................................................................................ 11  
6 Secure Communications........................................................................................................ 12  
   6.1 Encryption of Data in Transit......................................................................................... 12  
   6.2 Encryption of Data at Rest ............................................................................................ 12  
   6.3 Network Ports Usage...................................................................................................... 10  
7 Secure Software Development............................................................................................... 10  
   7.1 Input Validation.............................................................................................................. 10  
   7.2 Fail Safe ....................................................................................................................... 10  
   7.3 Trust Boundaries .......................................................................................................... 10  
8 Assumptions, Constraints, and Risks.................................................................................... 10
8.1 Assumptions .................................................................................................................. 10
8.2 Intrusion Detection and Prevention ............................................................................. 11
8.3 Constraints ................................................................................................................... 11
8.4 Risks .............................................................................................................................. 11
9 Requirements Traceability .............................................................................................. 11
10 Deliverable Format ......................................................................................................... 11
11 Deliverable Acceptance Criteria ..................................................................................... 12
12 Deliverable Schedule ....................................................................................................... 12
13 Appendices 13
   13.1 Appendix A: Deliverable Record of Changes ........................................................ 13
   Appendix B: List of Acronyms ....................................................................................... 13
   13.2 Appendix C: Glossary ............................................................................................. 15
   13.3 Appendix D: MECT Checklist ................................................................................. 16
   13.4 Appendix E: Critical Success Factors ..................................................................... 16
14 Other Information ............................................................................................................. 17

List of Tables

Table 1: Network Ports Usage............................................................................................. Error! Bookmark not defined.
Table 2: Deliverable Acceptance Criteria ........................................................................... 12
Table 3: Deliverable Schedule ............................................................................................ 12
Table 4: Record of Changes ............................................................................................... 13
Table 5: List of Acronyms ................................................................................................ 13
Table 6: MECT Checklist .................................................................................................. 16
Table 7: Critical Success Factors ....................................................................................... 16

List of Figures

Figure 1: Security Design Architecture............................................................................. 3
Figure 2: MMISR IdAM Framework................................................................................... 8
1 Introduction

The infrastructure of the SI Platform and all the integrated modules will be designed to provide security throughout the entire information processing life cycle. Each aspect of the implemented security measures is in accordance with the Minimum Acceptable Risk Safeguards for the Exchanges (MARS-E) v2.0 suite of controls. These controls collectively help to ensure that the confidentiality, integrity, and availability of data is maintained. This Security Design Document (SDD) will provide a high-level overview of how security will be designed into the SI Platform infrastructure.

The purpose of the SDD is to demonstrate how and where security controls will be implemented and how they relate to the system’s overall architecture. Security will be covered in each of the following areas:

- Security of Physical Premises
- Identification (ID), Authentication, and Authorization
- Logging and Auditing
- Encryption
- Secure Communications
- Secure Software Development

The SI Contractor will work collaboratively with the modular contractors to ensure that the security design is integrated cohesively and seamlessly into the existing infrastructure. This will be accomplished through meetings and documentation reviews and updates throughout the module’s onboarding and deployment process.

1.1 Overview

The New Mexico (NM) Health Services Division (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 Audience

The intended audience for this plan includes the NM HSD stakeholders, the module contractors, and the SI contractor team.

1.3 Purpose

The purpose of this plan is to demonstrate that security controls have been considered and will be implemented throughout the SI Platform in accordance with the MARS-E v2.0 controls. It is intended
to provide a high-level overview of the defense in depth security measures that will be incorporated into the design of the SI Platform.

2 Security Design Overview

This section will provide an overview of the SI Platform to include the system’s purpose, description, security architecture, and the applicable standards.

2.1 System Security Description

This new system approach requires the implementation of defense in depth to ensure that the data that is created, collected, processed, accessed, and maintained is protected throughout the data life cycle. The SI Platform will utilize and adhere to the controls as outlined in the MARS-E v2.0. This standard prescribes safeguards across 26 control families that cover protections spanning from the physical environment to the network perimeter and within the application layer. The subsequent sections below will provide a high-level overview of how each of these controls will be satisfied throughout the SI Platform infrastructure.

2.2 Security Architecture

The SI Platform is composed of functional segments that include the infrastructure, operating system/network, and the platform. The security architecture is comprised of software and hardware technologies in each of these functional areas that implement the required security safeguards per the MARS-E v2.0 best practices. The security measures for each of these areas are described at length below.

2.2.1 Infrastructure/Network

At the core of the Infrastructure is the Dell EMC VxRack Hardware Platform. The VxRack resides in the Department of Information Technology (DoIT) data center. The VxRack is connected to the network via Cisco switch routing which maintains port security and sits behind the Palo Alto next-generation firewall. At the outer perimeter of the DoIT Network sits an additional next-generation firewall that employs a deny all permit by exception for added protection of traffic entering the network. The VMware vSphere installed and configured in the management workload of the VxRack helps in virtualizing the hardware that is comprised of Computer Processing Unit (CPU), memory and storage on the virtual workload. At the base of the hardware is the ESXI hosts configured in a VMware Cluster within a datacenter of the vSphere. Virtual Machine (VM) hosts the Operating Systems (OS) along with the application and the directory service groups provide separation from management and security-related functionalities. An anti-virus is run on each of the VMs.

The proposed future state includes the NSX component. The NSX contains virtualized networking components including the Edge Services Gateway. The Edge Services Gateway provides firewalls, routers, switches, Dynamic Host Configuration Protocol (DHCP), Virtual Private Network (VPN), and load balancing to protect the perimeter of the SI Platform and ensure secured communications within and outside of the network.
2.2.2 Operating System/Network

At NMHSD each environment will be tagged with its respective VLAN and network segments at the vSphere level and no servers can be provisioned across networks unless authorized. We will be using the present Palo Alto firewall as the default gateway for all the servers on which the Layer 3 network are configured and traffic across subnets flow through the configured rules which gives a high level of security for the traffic flow.

At the operating system level, the vSphere is the compute component of the VxRack that provides the virtual machines. Each of these machines will carry a gold image of the Red Hat Enterprise Linux (RHEL) operating system (version 7.6). The Windows Server Operating system 2016 will be used as the platform for some of the Shared Services capabilities. Gold images for both of these operating systems will be created by patching and configuring the platforms to meet the United States Government Configuration Baseline (USGCB) standards and the Internal Revenue Service (IRS) Safeguard Computer Security Evaluation Matrix criteria. Both the RHEL and Windows operating systems have an Evaluation Assurance Level of 4+ for the operating system protection profile, thus it meets the MARS-E v2.0 security requirements such as process isolation.

2.2.3 Platform

The SI Platform will have an Oracle Fusion Middleware (OFMW) based Enterprise Service Bus (ESB) and Service Oriented Architecture (SOA). The ESB is a Message-Oriented Middleware (MOM) solution that will act as the backbone of SI Platform, enabling modules of disparate functionalities and technology platforms to communicate with each other. The ESB will communicate between modules via one of four connection methods:

- Web services (via Hypertext Transfer Protocol Secure [HTTPS]-port 8443).
- Database adaptor (via Open Database Connectivity [ODBC]-port 1433 and Java Database Connectivity [JDBC]-port 1433).
- Managed File Transfer (MFT) (via File Transfer Protocol/Secure [FTP/S]-port 990 or 21)
- Extract Transform Load (ETL).
Communication between any two modules in MMISR will occur through Web Services or database connections, via Application Programming Interface (API) deployed on ESB. It can also occur via file transfer or ETL. The Service bus utilizes the Oracle Web Services Manager (OWSM). The OWSM is a component of the OFMW and will be configured to manage security policies and propagate identities across web services. OWSM policies will require that the systems that interact with ESB have proper authentication and can only access the authorized resources. It ensures that the messages entering or leaving the ESB platform are encrypted to prevent data leakages and maintain the integrity of the messages. Data traversing between nodes within ESB will be encrypted via Transport Layer Security (TLS) v1.2.

2.2.4 Enterprise Shared Services

Enterprise shared services are comprised of the following set of services:

- **Enterprise Document Management (EDM):** EDM is a set of enterprise-level APIs that expose functionalities of the document management tooling: Perceptive Content.
- **Enterprise Communication Management (ECM):** ECM is a set of enterprise-level APIs that expose functionalities of the communication management tooling: OpenText Extream.
- **Enterprise Address Verification Service (EAVS):** EAVS is a set of enterprise-level APIs that expose functionalities of Address Standardization, Validation and Verification tooling: SAP Data Services.
- **Enterprise Data as a Service (EDAS):** EDAS is a set of enterprise-level APIs that expose functionalities of the Master Data Management (MDM) implementation.
- **Enterprise Identity Access Service (EIAS):** EIAS is a set of enterprise-level APIs that exposes Identity and access related APIs to provide a robust security framework that can be used by any HHS 2020 enterprise application for application security. The EIAS is not covered in this section but addressed as part of ESB security design.

The Enterprise Utility Service is hosted as a shared service to be consumed by multiple MMISR modules including UPI and Business Process Outsourcing (BPO) modules like DS, FS, and BMS. Every communication between any of the MMISR module and the ESS happens through ESB. These shared services are not exposed to any external consumers or agencies.

- **Transport Layer Security:** The communication between the ESB and all the ESS components are encrypted using one-way SSL. Here, the ESB validates the certificate of the ESS component server. This validation is done to make sure that it is the expected server, i.e. no Man in the Middle (MITM) attack.
- **EDM Transport Security:** The Perceptive Content’s Integration server works on top of Apache Tomcat web server. The keystore configuration and certificate import operations are the same as what is followed for any web server. The ESB layer working along with the OWSM component will interact with the Perceptive Content’s Integration Server using one-way SSL security mechanism.
- **ECM Transport Security:** The Communication Server of OpenText Exstream will be configured to receive HTTP calls from ESB. The ESB layer working along with the OWSM component will interact with the OpenText Exstream using one-way SSL security mechanism.
- **EAVS Transport Security:** The SAP data services natively support several of security mechanism like Basic, Authorization Header (Token or key based), and OAuth 2.0 among
others. The ESB layer working along with the OWSM component will interact with the SAP DS Access Server using one-way SSL security mechanism.

- **EDAS Transport Security:** In case of the EDAS, MarkLogic is the data store and MarkLogic Server uses Federal Information Processing Standards (FIPS)-capable OpenSSL to implement the Secure Sockets Layer (SSL v3) and Transport Layer Security (TLS v1.2) protocols. When the MarkLogic Server is installed, FIPS mode is enabled by default and SSL RSA keys are generated using secure FIPS 140-2 cryptography. This implementation disallows weak ciphers and uses only FIPS 140-2 approved cryptographic functions. Note that the FIPS mode can be enabled or disabled on a running system. If FIPS mode is enabled or disabled on a running system, the OpenSSL library is reconfigured appropriately without requiring a server restart. When the FIPS mode setting changes and secure XDQP is configured, all XDQP connections are dropped and reestablished.

- **Data Security:** The three ESS components, SAP Data Services, Perceptive Content, and OpenText Exstream use Oracle RAC as the data store. The data stored in the database is secured using Oracle Advanced Security feature called Transparent Data Encryption (TDE), where the complete database is encrypted. The ESS applications and users authenticated to the database continue to have access to application data transparently with no application code or configuration changes required. Attacks from OS users attempting to read sensitive data from tablespace files and attacks from thieves attempting to read information from acquired disks or backups are denied access to the clear text data.

- **EDAS Data Security:** The EDAS implementation is MarkLogic based, and the security details including cluster configuration, role-based security, and document level security explained in Section 5.4 applies to EDAS as well.

### 2.2.5 Disaster Recovery

A Federal Risk and Authorization Management Program (FedRAMP) approved Cloud Service Provider (CSP) will be used for the disaster recovery site. As a FedRAMP approved CSP, all applicable MARS-E v2.0 controls will be assessed and validated by an independent Third-Party Assessment Organization (3PAO). The physical security measures that are in place will be outlined in the FedRAMP package.

### 2.3 Applicable Standards

The following section references the applicable federal and State standards that are used as governance for the security design. These standards are:

- Accessibility standards established under Section 508 of the Rehabilitation Act, or standards providing greater accessibility for individuals with disabilities, and compliance with federal civil rights laws.

- FedRAMP certification in case any SI Platform component or service is in the Cloud. The current Oracle Government Cloud (OGC) is not FedRAMP-approved as of now. Oracle is working towards obtaining FedRAMP certification for OGC. The Disaster Recovery (DR) environment is going to be hosted in the Cloud.

- National Institute of Standards and Technology (NIST) Special Publication 800-131A, Revision 1.

- Health Information Technology for Economic and Clinical Health (HITECH) Act.
- Health Insurance Portability and Accountability Act (HIPAA) of 1996.
- Internal Revenue Service (IRS) Publication 1075.
- Center for Internet Security Benchmarks (https://www.cisecurity.org/cis-benchmarks/).
- Payment Card Industry Data Security Standard (PCI DSS).
- Emergency Department Information Exchange (EDIE) Records System Standards.
- National Information Exchange Model (NIEM).

3 Security of Physical Premises

The SI Platform system will be located at the State of NM DoIT primary data center. The DoIT primary data center has the following physical safeguards in place to protect data and associated transactions and functions:

- Data center visitors must properly complete a sign-in sheet at the guard’s station with date, arrival and exit time, name, organization, signature, form of ID, purpose of visit and person visiting. Escorts are always required for all visitors with access only to areas that are specific as to the reason for their visit.

- DoIT’s Santa Fe data center building has one main entrance that is accessible between 7am-6 pm. One dock and one backdoor entrance are only accessible by badge between 7 am-6 pm. After 6 pm, the building is secured, and the only way to enter is by phoning the guard from the front locked door. Some eligible staff may badge in after hours for system maintenance. The DoIT data center has security guards 24 hours a day, seven days a week, and 365 days a year. All DoIT and other State agency employees and vendors/contractors must always carry displayed picture badges.

- In the data centers, the badge system is located at points of egress/ingress. This enables an audit trail that is logged for auditing history at each door. Some doors do not allow you in or out (Anti-pass back) if you follow someone through, your badge will suspend.

- Data center access is more restricted than the office areas. Data center access requires badge card readers for entry and exit, and biometric readers for access. Closed Circuit Televisions (CCTVs) record activity in the DoIT data center building at each door and each grid view on the data center floor.
• The Disaster Recovery site will be hosted in a FedRAMP approved cloud service provider. All Physical Environmental (PE) controls per the MARS-E v2.0 will be met.

4 Identification, Authentication, and Authorization

This section will describe how services from the SI Platform and the other integrated modules will be accessed and deployed to the end user and/or other services acting on behalf of the end user. This will include:

• Identification and Authentication
• Access Management (Authorization) and End User Data

4.1 Identification and Authentication

The SI Platform will have the capability to uniquely identify a user and authorize access to certain applications based on the user’s identity through an Identify Management (IdAM) Solution. Identity and Access Management will manage authentication into the MMISR network. The IdAM platform serves Authentication, Multifactor Authentication, Federation, Provisioning, De-Provisioning, Delegated Administration, Password Management services and coarse-grained authorization. Course grained authorization is made at the perimeter of the network. The fine-grained authorization for protected resources is managed by the role-based access policies defined within each of the applications.

4.1.1 Web Services Authentication

Some of the communication between different MMISR applications is invoked through Web Services and APIs deployed on ESB. That communication requires both authentication and verification of the identity, and authorization and determination of permission to access data or services. ESB enforces these security controls using custom OWSM policies that communicates with IdAM along with One-Way or Two-Way SSL Certificates.

4.1.2 UPI Portal Authentication

The diagram below provides a view of the MMISR IdAM framework.
4.1.2.1 The Access Control Gateway

This layer is the entry point for UPI Portal users. It provides web-based access to the portal application and authenticates user access to the system. Oracle Access Manager Agent (Web Gate) will be deployed on UPI Web servers and act as a policy enforcement agent. Web Gate intercepts all the incoming requests to the UPI and performs a check whether the request requires authentication or not. Web Gate is integrated with Oracle Access Manager.

4.1.2.2 Authentication and Coarse Grain Authorization

This layer provides the Authentication, Access, and Federation for the users. The authentication and coarse-grain authorization decisions will also be taken from the functional COTS products. The coarse-grain access control restricts the end-user access to application/activities. This is typically a restriction based on the resource (hostname) or URI in the URL.

In addition to above, this layer is also responsible for Multi Factor Authentication (MFA) SSO within the MMISR applications as well as Federated SSO with the supporting external applications.

The authentication and coarse-grain authorization functionality of the applications is realized through the Oracle Access Manager (OAM) Component and its extensions.

4.1.2.3 Fine Grain Authorization

The fine-grain access control restricts the end-user access to specific data elements within the application. This restriction may prevent certain content from appearing on a page based on a user’s application defined role. Once Oracle IAM has validated the user credentials, the control is passed on to the respective applications to address the fine-grained authorization requirements.

4.1.2.4 Data Repository
The IdAM platform maintains the user repositories as well as security, policy, reporting, and session data at the back end. This layer is responsible for providing fast access to the data while maintaining the integrity and security that is required for handling sensitive eligibility information.

The user store component (Lightweight Directory Access Protocol (LDAP) based) provides:

- Centralized user account store for Individuals (OUD)
- Proxy services for accessing the Employee User Store (Active Directory)

The individuals’ data is stored in a centralized secure LDAP server i.e., Oracle Unified Directory (OUD). The passwords will be stored in the hashed (3DES+SSHA) algorithm and is not readable by anyone.

The directory server will implement attribute level Access Control Instructions (ACI) for directory server data. These ACIs will provide fine-grain access to directory server attributes. ACIs will utilize the native directory server role mechanism. Normal user access will be limited to self, minus security, and operational attributes. The application IDs will be updated with the necessary roles to provide access to the attribute.

The attributes will be aggregated in the ACIs so that they are grouped in classifications based on sensitivity and use. This generic approach still allows access to some attributes which may be unnecessary to an application, but it is assumed that the applications will only access attributes it requires. This will still reduce exposure of attributes to applications which are not allowed access to them.

All communication between OAM to OVD to OUD will be in SSL mode and use the self-signed server certificate.

### 4.1.2.5 Federation

In MMISR, Security Assertion Markup Language (SAML) is used as the Federation protocol, which is an XML-based protocol for exchanging security information between disparate entities. Some of the existing HSD applications will be integrated into MMISR systems using SAML based Identity Federation.

Depending on the user type, either Active Directory Federation Service (ADFS) or Oracle Identify Federation (OIF) will be configured to generate a SAML token. This SAML token will have the user and application attributes that will grant the user seamless access to MMISR applications and Services. The SAML assertions will be signed and encrypted with X509 certificates so as to make them tamper proof.

OIF, in turn, is integrated with OAM to delegate the authentication to centralized SSO solution implemented as part of MMISR IdAM platform.

### 4.2 Access Management and Non-Privileged HSD User Data

The IdAM framework includes Oracle Access Management Identity Federation engine and is used for providing Single Sign-On to HSD non-privileged employees accessing UPI. A federated trust will be configured between the Employee Active Directory Federation Service (ADFS) and the Oracle Identity Federation (OIF) with ADFS acting as the Identity provider and OIF as the service provider. Similarly, the OIF server can work with any number of Identity providers or service providers.
For employee access to UPI, when a state employee is accessing a resource protected by Oracle Access Manager such as UPI, Oracle Identity Federation redirects the user to State ADFS for global authentication. ADFS will obtain credentials, authenticate the user, and redirect the user back to the Oracle Identity Federation server instance - which retrieves the asserted identity from the ADFS and redirects the authenticated user to the access manager which provides access to UPI Portal. Some of the existing HSD applications can also participate in the Federated SSO provided by the IdAM Federation services.

MMISR IdAM federation supports the transport and receipt of request and response messages using either the Security Access Markup Language (SAML) 2.0 specifications, SAML 1.1, OpenID 2.0 or WS-Federation 1.1. SAML uses an eXtensible Markup Language (XML) framework to define a simple request-response protocol in order to achieve interoperability between different applications using SAML assertions. SAML requester sends a SAML Request element to a responder. Similarly, a SAML responder returns a SAML Response element to the requester. SSO and Federation relies on SAML artifacts and assertions to relay authentication information.

Identity data transported using the SAML 2.0 in MMISR is secured using the following specifications:

- All outgoing Assertions will be signed.
- All outgoing requests/responses not containing Assertions will be signed.
- The signing certificate will not be included in the messages.
- Identity Federation (acting as the IdP) will not require signatures on any messages except when specified in the SP Partner metadata.
- Name IDs, attributes, and assertions will not be encrypted.
- The hashing algorithm for signatures will be configured to use SHA-256.

SAML token will have the user and application attributes that will grant the user seamless access to MMISR applications and Services. The SAML assertions will be signed and encrypted with X509 certificates so as to make it tamper proof.

### 4.2.1 Server Authentication – Web Services

Transport Layer Security (TLS) 1.2 is used to authenticate the service provider to the service consumer and verifies the server certificate is issued by a trusted provider, is not expired, is not revoked, and matches the domain name of the service.

### 4.2.2 User Authentication – Web Services

User authentication verifies the identity of the user or the system trying to connect to the service. Such authentication is usually a function of the container of the web service.

- Internal web services: Username/Password in Simple Object Access Protocol (SOAP) header for SOAP web services, HTTP basic for Representational State Transfer (REST) web services are implemented to achieve user authentication. The authentication mechanism and credentials are integrated with IdAM.
- External web services: Client Certificate authentication is implemented to achieve user authentication.
5 Logging and Auditing

The SI Platform will employ Splunk for centralized auditing and logging solutions to capture relevant security events that could be utilized as evidence or trace the steps of a security incident. Across the architecture of the SI Platform audit trails will be logged and temporarily stored in the respective databases and then pushed to Splunk. The audit information will capture information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, and the outcome and identity of any individuals or objects associated with the event. Specifically, the SI Platform will provide the following auditing capabilities:

- All applicable auditable events per the MARS-E v2.0 AU-2 control.
- Configuration changes: The ESB platform provides an administrative console to view and access the history of configuration changes to the ESB application.
- User profile change and User access activity: The ESB platform keeps track of the users who log into the application and stores their session details, such as the message exchanges and services consumed.
- Message flows: The ESB platform creates persistent files of the messages that flow across the pipeline.

Log Insight is a part of the VMware/vRealize suite of tools. This module will provide universal log collection, powerful log analytics, and enterprise-class scalability in real-time, to analyze the log across all the components within the SI Platform virtual infrastructure. Artificial Intelligence is built in the vRealize suite for predictive and proactive remediation as the logs are collected and analyzed, using vRealize for performance and capacity.

Storage for Oracle auditing is temporarily held on each source database and later pushed to Splunk. The Oracle Enterprise Manager monitors the space on each database server and will alert the DBA to shortages on tablespace allocations. All audit logs will have view only access to maintain integrity of the log files.

Internal system clocks generate time stamps for audit records and are mapped to Coordinated Universal Time (UTC). Audit trails also support the log/audit requirements of regulations such as, the HIPAA §164.308(a)(1)(ii)(D): Security Management Process to implement policies and procedures to prevent, detect, contain, and correct security violations, including, implementing procedures to regularly review records of information system activity, in addition to the applicable standards listed above.

The SI team reviews and analyzes information system audit records daily through the Splunk console for indications of inappropriate or unusual activity. Specifically, the team will monitor the following:

1. Initialization sequences, logons, and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period.
2. Network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period.
3. Suspicious activity or suspected violations on the information system, and report findings to appropriate officials and take appropriate action.
4. Automated utilities to review audit records at least once weekly for unusual, unexpected, or suspicious behavior.

5. Administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.

### 6 Secure Communications

Cryptographic mechanisms will be used to maintain the confidentiality and integrity of data in transit and at rest. This section will describe how those mechanisms will be incorporated within the SI Platform infrastructure and how they will be used to protect the data that is collected, used, transmitted, and stored.

#### 6.1 Encryption of Data in Transit

The SI Platform ensures all environments that hold data subject to special classifications other than public are encrypted to protect all data being exchanged with external and internal entities. This includes data both in transit and at rest and traversing to and from the DR site.

All types of transmission of data which includes client-to-server, server-to-server communication as well as any data transfer between the SI Platform and the third-party systems is encrypted in MMSIR as follows:

- Web traffic is encrypted using strong security protocol, Transport Layer Security (TLS 1.2+).
- The connection between the database and application is encrypted using SSL.
- Batch file transfers such as EDI communication, file transfers to and from Federal, local, or State agencies are secured by using Secure File Transfer Protocol (SFTP).
- ESB messages will use SOAP/REST over HTTPS protocol for secure web services communication.

#### 6.2 Encryption of Data at Rest

Data at rest includes data stored physically in any digital-form such as databases, spreadsheets, archives, tapes, offsite backups.

- Sensitive data stored in the database is secured using Oracle Advanced Security TDE), where the complete database is encrypted. It stops attackers from by-passing the database and reading sensitive information from storage by enforcing data-at-rest encryption in the database layer.
- Transparent Data Encryption fully supports Oracle Multi-tenant. When moving a Pluggable Database (PDB) that contains encrypted data, the TDE master keys for that PDB are transferred separately from the encrypted data to maintain proper security separation during transit.
- Sensitive data stored in archives, tapes and offsite-backups are also encrypted using FIPS compliant encryption algorithm.
• The cloud service provider will be FedRAMP certified and thus, by requirement, will use FIPS 140-2 compliant algorithms.
6.3 Network Ports Usage

7 Secure Software Development

This section will describe the safeguards that will be employed throughout the development of the SI Platform to ensure the confidentiality, integrity, and availability of the information is maintained and secured.

7.1 Input Validation

Input validation will be performed to ensure that any data supplied by a user will be validated to ensure that only properly formed data enters the system boundary. Data validation will occur through whitelisting expected values and syntaxes and will help to prevent injection attacks and memory leakages.

7.2 Fail Safe

The SI Platform utilizes active-passive configurations on its boundary protection devices (such as the routers and the firewalls), the configurations are synchronized, and the cabling is mirrored on both devices. In the event of a hardware or network failure (per port) the devices are configured to failover to the passive standby device. If both devices fail in the event of a major operations failure, then the traffic is not able to be passed thru the devices to the subnets and logical subnetworks.

7.3 Trust Boundaries

The Integrated Platform has three trust boundaries that include the access or presentation zone, the platform, and the data zone. Each trust boundary is protected by the Palo Alto firewall will provide protection for external (North-South) traffic, and in addition, provides protection for internal (East-West) traffic across subnets.

8 Assumptions, Constraints, and Risks

8.1 Assumptions

This subsection documents an initial set of assumptions for configuration and continuous integration activity, which may be updated over time. Sample assumptions:

- Significant deviations from stated implementations will not be needed due to things such as hardware/software incompatibility.
- There will not be any significant changes to the MARS-E v2.0 or any other federal and state requirements that would require changing the stated implementation.
8.2 Intrusion Detection and Prevention

The Palo Alto is a next-generation firewall that will provide traditional stateful firewall capabilities along with Deep Packet Inspection (DPI). DPI will check for malicious code and drop any suspicious traffic. Additionally, the Palo Alto firewall has a built-in Intrusion Protection System that will be used to monitor the network, detect known virus signatures, and drop those packets. It will also drop suspicious and malicious traffic.

8.3 Constraints

This subsection describes an initial set of constraints, which may be updated over time.

- None identified at this time

8.4 Risks

This subsection describes an initial set of risks specific to the Security1 – Security Approach. It is not a restatement or selection of project risks. All project risks will be updated and managed per the Risk Management Plan.

Sample risks:

- None identified at this time

9 Requirements Traceability

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

- Request for Proposal (RFP)
  - Page 112
  - Section 2.2.1.12
  - Section 2.2.2.8

- Proposal
  - Page 46
  - Page 45 Section 1.3.4.1.11
  - Page 89 Section 1.3.7.1
  - Page 193 Section 2.2.42

- Statement of Work (SOW)
  - Security3

- HSD Decision Log Entry #31:
  - PMO37 CCIS Deliverable Scope Change

10 Deliverable Format

This deliverable will be submitted as a Microsoft Word document. Its estimated size is 50-75 pages.
11  Deliverable Acceptance Criteria
The deliverable will include Deliverable Acceptance Criteria in the following form.

Table 1: Deliverable Acceptance Criteria

<table>
<thead>
<tr>
<th>Item Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deliverable includes items in Section 2.4</td>
</tr>
<tr>
<td>2</td>
<td>Deliverable meets requirements in Section 2.5</td>
</tr>
<tr>
<td>3</td>
<td>Deliverable meets all requirements in Section 3</td>
</tr>
<tr>
<td>4</td>
<td>Deliverables meets all quality assurance standards.</td>
</tr>
<tr>
<td>5</td>
<td>Deliverable meets quality checklist, including style guide check list item. Link to checklist: Shared Resources folder on SharePoint</td>
</tr>
</tbody>
</table>

12  Deliverable Schedule
The Deliverable Schedule follows.

Table 2: Deliverable Schedule

<table>
<thead>
<tr>
<th>Steps</th>
<th>Completion Date</th>
<th>Description</th>
<th>Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>02/22/19</td>
<td>Complete Draft</td>
<td>TPGSI Team Lead</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Complete Review and Provide Feedback</td>
<td>NM HSD</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Incorporate comments into Final</td>
<td>TPGSI Team Lead</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Final Deliverable Approved</td>
<td>NM HSD</td>
</tr>
</tbody>
</table>
13 Appendices

13.1 Appendix A: Deliverable Record of Changes

The deliverable will include a record of changes in the following form.

**Table 3: 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>02/22/2019</td>
<td>Tonya Love</td>
<td>Draft Created</td>
</tr>
<tr>
<td>V0.2</td>
<td>4/5/2019</td>
<td>Tonya Love</td>
<td>Edits made across entire document</td>
</tr>
</tbody>
</table>

Appendix B: List of Acronyms

The deliverable will include a List of Acronyms in the following form. For a comprehensive, project-wide list of acronyms, consult the Master Acronyms list on the SI Contractor team at [Shared Resources on SharePoint](#).

The following is a list of all acronyms used in this document.

**Table 4: List of Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADFS</td>
<td>Active Directory Federation Service</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>BPO</td>
<td>Business Process Outsourcing</td>
</tr>
<tr>
<td>CCTVs</td>
<td>Closed Circuit Televisions</td>
</tr>
<tr>
<td>CMS</td>
<td>Centers for Medicare and Medicaid Services</td>
</tr>
<tr>
<td>CPU</td>
<td>Computer Processing Unit</td>
</tr>
<tr>
<td>DEK</td>
<td>Database Encryption Key</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DoIT</td>
<td>Department of Information Technology</td>
</tr>
<tr>
<td>DPI</td>
<td>Deep Packet Inspection</td>
</tr>
<tr>
<td>EAVS</td>
<td>Enterprise Address Verification Service</td>
</tr>
<tr>
<td>ECM</td>
<td>Enterprise Communication Management</td>
</tr>
<tr>
<td>EDAS</td>
<td>Enterprise Data as a Service</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>EDIE</td>
<td>Emergency Department Information Exchange</td>
</tr>
<tr>
<td>EDM</td>
<td>Enterprise Document Management</td>
</tr>
<tr>
<td>EIAS</td>
<td>Enterprise Identity Access Service</td>
</tr>
<tr>
<td>ESB</td>
<td>Enterprise Service Bus</td>
</tr>
<tr>
<td>ETL</td>
<td>Extract Transform Load</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>FTP/S</td>
<td>File Transfer Protocol/Secure</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</td>
</tr>
<tr>
<td>HSD</td>
<td>Human Services Department</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>IdAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>IRS</td>
<td>Internal Revenue Service</td>
</tr>
<tr>
<td>JDBC</td>
<td>Java Database Connectivity</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</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</td>
</tr>
<tr>
<td>MDM</td>
<td>Master Data Management</td>
</tr>
<tr>
<td>MFT</td>
<td>Managed File Transfer</td>
</tr>
<tr>
<td>MITM</td>
<td>Man in the Middle</td>
</tr>
<tr>
<td>MOM</td>
<td>Message-Oriented Middleware</td>
</tr>
<tr>
<td>MMISR</td>
<td>Medicaid Management Information System Replacement</td>
</tr>
<tr>
<td>NIEM</td>
<td>National Information Exchange Model</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>ODBC</td>
<td>Open Database Connectivity</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>OFMW</td>
<td>Oracle Fusion Middleware</td>
</tr>
<tr>
<td>OIF</td>
<td>Oracle Identify Federation</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OWSM</td>
<td>Oracle Web Services Manager</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PDB</td>
<td>Pluggable Database</td>
</tr>
<tr>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>RHEL</td>
<td>Red Hat Enterprise Linux</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>SDD</td>
<td>System Design Document</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SI</td>
<td>System Integrator</td>
</tr>
<tr>
<td>SOA</td>
<td>Service Oriented Architecture</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>TDE</td>
<td>Transparent Data Encryption</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UCT</td>
<td>Universal Time</td>
</tr>
<tr>
<td>USGCBR</td>
<td>United States Government Configuration Baseline</td>
</tr>
<tr>
<td>UPI</td>
<td>Unified Processing Interface</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machines</td>
</tr>
</tbody>
</table>

**13.2 Appendix C: Glossary**

The deliverable will include a glossary of project-specific terminology is maintained by the SI Contractor team at [Shared Resources on SharePoint](#).
13.3 Appendix D: MECT Checklist

The deliverable will contain the Medicaid Enterprise Certification Toolkit (MECT) checklist items that correspond to Section 508 compliance.

Table 5: MECT Checklist

<table>
<thead>
<tr>
<th>Checklist ID</th>
<th>Requirement Text / System Review Criteria (SRC)</th>
<th>MITA Business Area Module Checklist Set</th>
<th>Business Process</th>
<th>Module Owner</th>
<th>CMS Guidance</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

13.4 Appendix E: Critical Success Factors

The deliverable will contain Programmatic Critical Success Factors:

Table 6: Critical Success Factors

<table>
<thead>
<tr>
<th>Checklist ID</th>
<th>Requirement Text / System Review Criteria (SRC)</th>
<th>MITA Business Area Module Checklist Set</th>
<th>Modular Owner</th>
<th>Business Process</th>
<th>CMS Guidance</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
14 Other Information

There is nothing to report at this time.