UHIP Security Approach

Phase 1 Health Information Exchange

The Rhode Island Unified Health Infrastructure Project(UHIP) initially received Authority to Connect to the Center for Medicare & Medicaid Services (CMS) Data Services Hub with an Interconnection Security Agreement (ISA) signed on 9/27/2013. The ISA establishes the Administering Entity's commitment to protect the data stored on the network and provide relevant technical and operational security requirements. In addition, commitment to compliance with the "Minimal Acceptable Risk Standards for Exchanges" (MARS-E) which implements the privacy and security requirements of 45 Code of Federal Regulation (C.F.R.) 155.260. The following supporting documentation accompanied the ISA in support of MARS-E 1 to receive the Authority to Connect (ATC):

- **Information Security Risk Assessment (ISRA)** - The Information Security Risk Assessment includes a system overview to provide a basic understanding of the system and its interconnections, and describe the overall system security level. Additionally, the RA Report contains a list of system threats and vulnerabilities; an evaluation of current security controls to safeguard against the identified threat/vulnerability pairs and the resulting risks levels; and the recommended safeguards to reduce the system's risk exposure with a revised or residual risk level once the recommended safeguards are implemented.

- **Privacy Impact Assessment (PIA)** - Identify the specific types of sensitive information that the AE will collect, store, use, process, disclose, or disseminate while administering an Affordable Care Act (ACA) State-based Marketplace (SBM), Medicaid, Children's Health Insurance Program (CHIP), or Basic Health Program (BHP), analyze the privacy risks associated with maintaining that information, and subsequently document the results of the analysis.

- **System Security Plan (SSP)** - The SSP is the key tool for describing an AE's IT security and privacy environment for IT systems and for documenting the implementation of security and privacy controls for the protection of all data received, stored, processed, and transmitted by the ACA AE's IT systems and supporting applications. AEs are required to complete the SSP and document their compliance with mandates of the ACA legislation and Department of Health and Human Services (HHS) Regulations.

- **Third party Independent Security Assessment Report (SAR)** - Third Party security assessment with and audit on compliance with MARS-E 2 controls and recommended corrective actions.

- **Plan of Actions and Milestones (POAM)** - A corrective action plan resulting from the analysis of the security controls by third party vendors, vulnerability scans, security plan reviews etc. Deficiencies are evaluated for impact and likelihood to determine security risk level and schedule priority.

- **Information Exchange Agreement (IEA)** - Terms, conditions, safeguards and procedures under which CMS will exchange certain information with State Exchanges.

- **Computer Matching Agreement (CMA)** - Terms, conditions, safeguards and procedures under which CMS will exchange certain information with Administering Entities using FDHS.

- **IRS Safeguards Security Report (SSR)** - The report reflects the agency's current environment for the receipt, storage, processing and transmission of FTI.

- **SSA Security Design Plan (SDP)** – Security Design Plan for approval for access to SSA-provided data. The SDP must document compliance with SSA's Systems Security Requirements.

An independent third party vendor performed a system audit of the UHIP system in September 2013 and recommended current and future activities to reduce security risks. These action items were captured on the Plan of Actions and Milestones and completed on a schedule associated with risk.

Additional audits and reviews were performed by the IRS (7/2014) and the State of Rhode Island Office of the Auditor General (6/2015) single audit. The Social Security Administration performed an onsite certification of the UHIP application during the summer of 2015. Additionally, a SOC 1 Type 1 audit was performed.

The System Security Plan describes the robust security architecture and security processes in place including:

- System vulnerability scanning – external and internal penetration tests, source code, network
- QRadar - security logging and monitoring of the network and system
- TIM/TAM - access control management software

Phase 2

The State of RI followed CMS security protocol by submitting a Security Impact Assessment to CMS on 02/01/2016 informing them of the significant system change to Implement an Integrated Eligibility System as Phase 2 of the Rhode Island United Health Infrastructure Project(UHIP). Because of the major changes to the UHIP system, **the state was required to get a reissuance of the Authority to Connect (ATC) from our federal partners**. Over the course of 6 months, a formalized evaluation of the security controls of the system was completed as follows:

- Reviewed System Security Plan to determine how specific security controls are implemented within the system and how the changes might affect the controls.
- Assessed the risk to determine the impact of the changes and if additional security controls are required.
- Tested and verified security functions after the change was made to determine if the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

The following supporting documentation were updated to reflect the system changes for phase 2 in support of MARS-E 2.0 compliance to receive the Authority to Connect (ATC):

- Information Security Risk Assessment (ISRA)
- Privacy Impact Assessment (PIA)
- System Security Plan (SSP)
- Third party Independent Security Assessment Report (SAR)
- Plan of Actions and Milestones (POAM)
- Information Exchange Agreement (IEA)
- Computer Matching Agreement (CMA)
- IRS Safeguards Security Report (SSR)

The following activities were completed in support of verifying the security architecture of UHIP:

On 8/1/2016 an independent third party vendor provided a comprehensive Security Assessment audit and provided independent testing of the MARS-E1 and MARS – E2 controls. The following scans were performed on internal and external network components:

- Web Application - both dynamic (actual attempts to hack in by a tool) and static analysis (source code review)
- Network Scanning/Penetration Tests
- Database Scanning

A recommendation of current and future activities to reduce security risks were captured on the Plan of Actions and Milestones (POAM) based on the results of the third party Security assessment report. A schedule to complete the items has been developed per risk rating. All high and critical issues were resolved prior to go-live and included operating system and software updates, code fixes, and configuration changes.

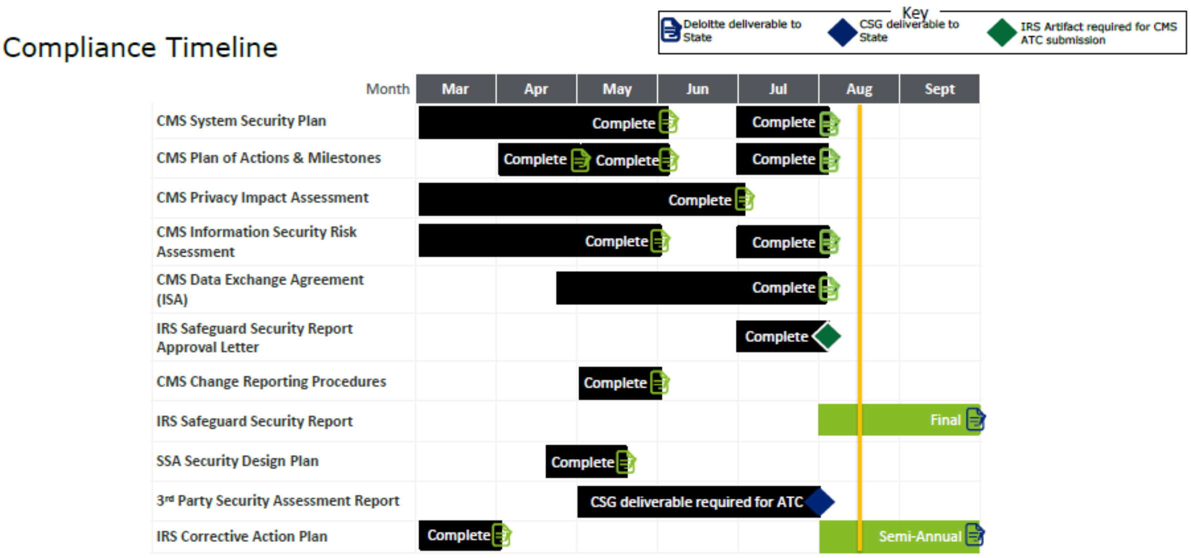
All system documentation was reviewed and updated with the new MARS-E2 requirements. CMS reviewed and approved the efficacy of the controls, risk assessment and actions plans on 9/9/2016 and provided the Interconnection Security Agreement and Authority to Connect to the CMS Federal Data Hub system.

On-Going:

To sustain the MARS-E 2.0 designation, the State is required to implement a continuous monitoring program as submitted to our federal partners. This consists of monthly and quarterly scans for:

- Web Application - both dynamic (actual attempts to hack in by a tool) and static analysis (source code review)
- Network/Penetration Tests
- Database scanning
- SSL Certificate testing

This monitoring is currently underway. Additionally, an AT101 audit is in progress and will be available in January 2017. The AT101 is based on the Deloitte controls only. A SOC 2 Type 1 (design and existence of controls that includes Deloitte and the State computer center) report will be available in February 2017 and a SOC 2 Type 2 (tested and corrected controls) to be available in third/fourth quarter of 2017. The SOC 2 Type 2 requires a period of time (6 months to a year) to elapse for controls to be corrected and retested. This additional audit will be executed on a more stable, mature UHIP application.



Compliance Timeline

Key

- Deloitte deliverable to State
- ◆ CSG deliverable to State
- ◆ IRS Artifact required for CMS ATC submission

Month	Mar	Apr	May	Jun	Jul	Aug	Sept
CMS System Security Plan			Complete		Complete		
CMS Plan of Actions & Milestones		Complete	Complete		Complete		
CMS Privacy Impact Assessment				Complete			
CMS Information Security Risk Assessment			Complete		Complete		
CMS Data Exchange Agreement (ISA)					Complete		
IRS Safeguard Security Report Approval Letter					Complete ◆		
CMS Change Reporting Procedures			Complete				
IRS Safeguard Security Report							Final
SSA Security Design Plan		Complete					
3rd Party Security Assessment Report				CSG deliverable required for ATC ◆			
IRS Corrective Action Plan	Complete						Semi-Annual