




Compliance and IT Security Update

MARYLAND
HEALTHBENEFIT
EXCHANGE




MHBE Governing Board Report October 18, 2016



MARYLAND HEALTH BENEFIT EXCHANGE

Audits Q4 2016	Status	Comments
Single State Audit FY2015	✓ Complete	Performed gap analysis, received subrecipient financial audit reports FY15, issued management decisions letters to Connector Entities. Complete.
Independent External Audit - Financial		CCIIO to determine how MHBE can comply with independent financial statement requirement. Develop internal controls for expenditure cycle.
Independent External Audit – Programmatic		Revise decertification procedures to comply with 45 CFR 155.1080 (b) and address segregation of duties, roles, and responsibilities. Designed and implemented processes to manually review cases to ensure is appropriate and timely redetermination. Automate process.
Privacy Impact Assessment PY16 and MARS-E v 2.0		Design, Revise and Implement new Privacy Controls section of the Minimum Acceptable Risk Standards for State-based Exchanges (MARSE v2.0) by June 30, 2017 to Include internal controls related to : <ul style="list-style-type: none"> • Authority and Purpose to Collect PII • Accountability, Audit and Risk Management • Data, Quality and Integrity • Data Minimization and Retention • Individual Participation and Redress • Security • Transparency • Use Limitation

Complete On-Track  Planned  At Risk 

Authority to Connect requirements for 2017 Summary	Status	Comments
Annual Security and Privacy Attestation	✓ Complete	Performed internal security self assessment of System Security Plan controls for years 1 and 2 of 3. Updated and implemented security controls consistent with Minimal Acceptable Risk Standards for Exchanges 2.0 (MARS-E 2.0) along with assessment including new Privacy Controls.
Privacy Impact Assessment (PIA)	✓ Complete	Completed Privacy Impact Assessment along with Privacy team. Opened findings and added to Agency Plan of Action and Milestones (POA&M).
Information Security Risk Assessment (ISRA)	✓ Complete	The MARS-E Risk Assessment addresses: <ul style="list-style-type: none"> Assurance of Confidentiality, Integrity, and Availability (CIA) of the system Effectiveness of implemented security and privacy controls Foreseeable internal and external threats to the information Likelihood of the threats exploiting on vulnerabilities Sufficiency of policies and procedures to mitigate the threats
Plan of Action and Milestones (POA&M)	✓ Complete	Completed Quarter 3 POA&M, Quarter 4 due October 31,2016.
IRS Safeguard Security Report (SSR)	✓ Complete	Completed Annual SSR, The SSR addresses all outstanding Actions identified by the IRS from prior years submissions.
IRS Corrective Action Plan (CAP)	✓ Complete	Completed Semi Annual Submission as an attachment to the SSR, next CAP due November 30 th , 2016.
System Security Plan (SSP)		Update System Security Plan to MARS-E 2.0 compliance. MARS-E 2.0 is the latest security standard required for state based exchanges. Target date: May 30 th , 2017.
Security Assessment Report (SAR)		Plan, Procure and deliver Third Party independent assessment of System Security Plan, Security and Privacy Controls consistent with the MARS-E 2.0. The triennial security and privacy control testing necessary for the renewal of an Authority to Connect (ATC). Target date: August 30 th ,2017.
Authority to Connect		Deliver Authority to Connect Package: includes System Security Plan (SSP), Security Assessment Report (SAR), Plan of Action & Milestones (POA&M), Signed Associate Information Security Agreement (ISA), Interconnection Security Agreement (ISA). Target Date: November 6, 2017