Compliance and Security Update

MHBE Governing Board
January 17, 2017

MARYLAND HEALTHBENEFIT EXCHANGE

Audits Q1 2017	Status	Comments
Independent External Audit - Financial		TORFP includes use of CAFR and audit of expenditures to meet 155.1200 (c). Expenditure internal control procedures created and under review
Independent External Audit – Programmatic		Revised carrier decertification procedures that comply with 45 CFR 155.1080 (b) and address segregation of duties, roles, and responsibilities under review. Termination of QHP enrollment to be automated.
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 : • 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
Audit Preparation FY2017		• GAO Eligibility and Enrollment – February • Independent External Audit PY 2016 – March • IRS 1075 Safeguards – April • Office of Legislative Audit – June

✓ Complete On-Track Planned At Risk

MARYLAND HEALTHBENEFIT EXCHANGE

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: • 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 4 POA&M, Quarter 1 due January 30,2017.
IRS Safeguard Security Report (SSR)	✓ Complete	Completed Annual SSR, The SSR addresses all outstanding Actions identified by the IRS from prior years submissions. Next SSR due May 31, 2017
IRS Corrective Action Plan (CAP)	✓ Complete	Completed second annual submission of CAP, next CAP due May 30, 2017
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 30th, 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 30th,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

✓ Complete On-Track Planned At Risk