Department of Veterans Affairs

Memorandum

Date: May 24, 2018

From: Deputy Assistant Secretary, Enterprise Program Management Office (005Q)

Subj: 150 day Authority to Operate (ATO) for Medical Care Collections Fund (MCCF) EDI TAS eBusiness Assessing

To: System Owner

1. Per the approval of the Deputy Assistant Secretary, Enterprise Program Management Office (EPMO) [the VA Authorizing Official (AO)], Medical Care Collections Fund (MCCF) EDI TAS eBusiness Assessing is granted an ATO to be in effect for 150 calendar days. This ATO will expire on October 21, 2018.

2. This ATO is issued to provide the system staff sufficient time to complete the necessary Assessment and Authorization (A&A) actions within the Governance, Risk and Compliance (GRC) tool, RiskVision.

a. Within 60 days of ATO issuance, this system requires the following actions:

i. Nessus Scan – Continue to receive monthly Nessus/NEWT scans. All findings should be mitigated and/or have a documented remediation strategy with expected mitigation date uploaded to Documents tab within RiskVision. A POA&M must be created to track the remediation progress.

ii. V&V Secure Code Review – All findings should be mitigated and/or have a documented remediation strategy with expected mitigation date uploaded to Documents tab within RiskVision along with the Secure Code Review results. A POA&M must be created to track the remediation progress.

iii. V&V Quality Code Review – All findings should be mitigated and/or have a documented remediation strategy with expected mitigation date uploaded to Documents tab within RiskVision along with the Quality Code Review results. A POA&M must be created to track the remediation progress.

b. Within 105 days of ATO issuance, this system requires the following actions:

i. Security Documentation – Ensure all system security documentation is completed and uploaded to RiskVision in accordance with the Accreditation Requirements within the Accreditation SOP, to include evidence for the security controls. The SSP from May 2018 has 31 ‘planned’ controls that need to be addressed. If controls are not fully implemented work to close the respective findings in RiskVision. Also, ensure that all findings and risks have a response provided for them within RiskVision, along with the details on financial/personnel resources required to resolve the finding. Refer to POA&M Management Guide located

on the OIS Portal for detailed instructions on creating and managing POA&Ms in RiskVision. Ensure current/accurate versions of the remaining security documentation, including the DRP, ISCP, PTA, and SA, are uploaded to RiskVision. Also, ensure all system security documentation is approved by the appropriate parties.

ii. Database Scan – If this project includes a database host, a full database scan must be scheduled with the VA-NSOC. Once the database scan results are received, all findings should be mitigated and/or have a documented remediation strategy with expected mitigation date uploaded to Documents tab within RiskVision. If a Database scan is not applicable, upload a word document to Documents tab explaining why a Database scan is not applicable.

iii. Penetration Test/Application Assessment – If this is an internet facing system, a penetration test/application assessment must be scheduled with VA-NSOC. Contact the Certification PMO at CertificationPMO@va.gov to request a penetration test/application assessment. Once the results are received, upload them to the documents tab within RiskVision. All findings should be mitigated and/or have a documented remediation strategy with expected mitigation date uploaded to Documents tab within RiskVision.

3. Retain a copy of this memorandum with all supporting security A&A documentation. Instructions to meet the ATO requirements can be found in the Accreditation Requirements SOP. If you have any questions, please contact Toby Rudik (System Owner) via email at Toby.Rudik@va.gov, or Bill James (Authorizing Official) via email at Bill.James@va.gov.

Bill James
Deputy Assistant Secretary
Enterprise Program Management Office (005Q)