



DEPARTMENT OF THE AIR FORCE

12 August 2020

MEMORANDUM FOR PLATFORM ONE, CHIEF INFORMATION SECURITY OFFICER (CISO)

FROM: Air Force Rapid Cyber Acquisition (RCA) Authorizing Official (AO)

SUBJECT: Cloud Native Access Point (CNAP) Fast Track Authority to Operate (ATO) Authorization Termination Date (ATD): **12 August 2023**

REFERENCES: (a) DoD Secure Cloud Computing Architecture (SCCA) Functional Requirements v2.9, 31 January 2017
(b) DoDI 8510.01 "Risk Management Framework (RMF) for DoD Information Systems", 12 March 2014
(c) Approval of Exception to DoD Policy for Development Security and Operations Native Cloud Access Point

1. As the Air Force Authorizing Official (AO) for Rapid Cyber Acquisition (RCA), I have assessed the risk for the Cloud Native Access Point (CNAP) having a residual risk as LOW and therefore grant an Authorization to Operate (ATO).
2. CNAP is a replacement for the standard Cloud Access Point (CAP), see reference c, that satisfies the requirements outlined in reference a to provide security for cloud native workloads operating at Impact Levels (ILs) 2/4/5 in both Amazon Web Services (AWS) GovCloud and Azure Government.
3. My determinization is based on the assessment of the security posture, identified risks, system specific requirements, proposed and agreed to mitigations, and all supporting documentation evaluated through the C2 risk assessment process conducted in accordance with AF and DoD guidance. This process is aligned with instruction for risk assessments in NIST SP 800-30 and takes into account the defined risk tolerance as identified in the accompanying documentation. This determination considers the extent to which the security risk remediations have been identified and any controls and/or mitigations have been implemented correctly, are operating as intended, and producing the desired level of protection.
4. This authorization is my formal declaration that appropriate system security measures and/or countermeasures for the identified risks have been properly implemented and that a satisfactory level of security is present for operations. This authorization is for this version only as documented in artifacts provided by the program and valid until the ATD specified. Operations outside the boundaries identified in the provided documentation will be just cause to revoke this authorization. Any changes or upgrades to the system baseline will need to be assessed through coordination with the C2 CRA Staff. A Plan of Action and Milestones (POA&M) is required to be maintained, reviewed quarterly, and progress reported to the C2 CRA Staff.

UNCLASSIFIED

UNCLASSIFIED

5. I maintain the authority to revoke this ATO based on lack of due diligence, non-compliance with aforementioned policies, and other security related infractions.
6. My point of contact for the CNAP environments is the Platform One ISSM Mr. Aaron D. Brown, he can be contacted via email at aaron.brown.66.ctr@us.af.mil or phone (719)749-1907.

DANIEL C. HOLTZMAN, HQE, USAF
Authorizing Official – Rapid Cyber Acquisition

UNCLASSIFIED