DEPARTMENT OF THE AIR FORCE

SUBJECT: Certificate to Field (CtF) for Padawan v1.x

References:

a) Continuous Authorization to Operate (cATO)
b) The Party Bus Ticket
c) National Institute for Standards and Technology (NIST) Special Publication 800-37, Rev 2, Risk Management Framework (RMF) for Information Systems and Organizations, September 2017
d) National Institute for Standards and Technology (NIST) Special Publication 800-53, Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
e) CNSSI 1253, Security Categorization and Control Selection for National Security Systems

1. A CtF has been granted for Padawan v1.x is an app that allows P1 customers who need a static site at anyenclave can have a set of pipeline templates hosted in Party Bus GitLab which help development teams deploy their static sites to the Mission Application Staging/ Production clusters. When get the CTF on the "Padawan system" once, then customers can focus on their static site development: content, look/feel, requirements. Party Bus provides the hosting and DNS so the customers can focus on their site instead of the infrastructure. Padawan-sync is the synchronizing code that periodically runs to pull site artifacts from the padawan-registry to create, update, or delete site content.

Component Name:	Component Description:
Padawan - Sync	The hosting mechanism is essentially an NGINX container serving static files (html/css/js) over https.
Padawan – Umbrella	Padawan is a framework for Platform One customers to easily build, deploy, and host static sites.

2. Based on a formal software vulnerability evaluation conducted In Accordance With (IAW) reference b, page 10 with a determination that the software can be operated at an acceptable level of risk based on the submitted remediation and mitigation Plan of Action and Milestones (POA&M). The details, conditions and amplifying information of this CtF are as follows:

Applicable to:	Padawan v1.x (major version only)
Effective Date:	24 Jun 21
Expiration Date:	24 Dec 21
Evaluation Method(s):	Path to CtF Process
Authorized Use:	AF IS w/ AO approval

Conditions and Restrictions	a. This CtF applies to this major version only. b. CtF reissuance is dependent on continued mitigation efforts as specified in the POA&M. c. This CtF authorizes the use of the application on AF IS. d. Before the installation of software, ensure the software goes through the proper Configuration Control Board (CCB) process and complies with local organizational or program management office (PMO) configuration management policies. e. System Administrators will only install this version of this major release. f. Ensure all development/test code is removed before delivering software for installation on production systems. g. Any developer modification to the software configuration, significant fixes, operating systems supported, or new functionality may require recertification and must be reported to Platform One CISO and all Authorizing Official(s) IS containing the software prior to installing subsequent versions. h. The mission owner has exercised the option to exclude the use of Appgate to enforce comply-to-connect at IL4 for this software and has accepted the ensuing associated responsibility.
Additional Instructions	a. Although a CtF was granted, the software does contain vulnerabilities and the development team should continue to review all findings, work to address these findings and track efforts in the appropriate POA&M; especially any critical and high findings before submitting the next version for evaluation.

3. This CtF is not an Approval to Operate (ATO) but rather an evaluation of the inherent vulnerabilities in the software product and an assessment of risk in installation on AF IS systems. Implementation on specific AF IS systems is the responsibility of the Authorizing Officer (AO), PMO and/or System Owner and PM. The Installation approval decision should ultimately be based on a system-specific Security Impact Analysis (SIA) for initial major version installation on system/site with a current ATO. If the system/site does not currently have an active ATO, the CtF should be added to the RMF Body-of-Evidence (BoE) for consideration in the IATT/ATO decision.

4. This memo supersedes all others on the same subject.

HUSTON.MATTHEW.DEAN.1265844002

Digitally signed by HUSTON.MATTHEW.DEAN.1265844002
Date: 2021.06.24 13:40:21 -06'00'

MATTHEW D. HUSTON
Chief Information Security Officer