VERSION 1.0

04/27/2019

Mission Partner Onboarding Guidance

PROJECT HOSTS INC.
400 MAIN ST. CONNEAUTVILLE PA, 16406

TABLE OF CONTENTS

PURPOSE:

The Purpose of this document is to outline the responsibilities the mission partner will have to peform and act as a guide for the mission partner to be succesffully onboarded into the Project Hosts Federal Private Cloud DoD Environment (PJHFPCDoD) in the most seamless manner possible.

THE PROJECT HOSTS ADVANTAGE:

Project Hosts works with the mission partner every step of the way to ensure a easy transition to the cloud for your Cloud IT Project (C-ITP). Project Hosts has also already achieved its DISA Provisional authorization at Impact Level 5 saving mission partners from having to go through the DISA A&A process and dedicating personnel to that effortProject Hosts provides many services above and above offering a secure platform to deploy your application onto.. These services include:

- Assisting in the Assessment and Authorization process
  - Project Hosts Security compliance team will provide you with application level SSPs and documentation sets to include drafting Policies and Procedures for Customer Responsibility controls.
  - Project Hosts security compliance team is well versed in the eMASS system and all of the modules within eMASS and will manage uploading all of the required artifacts and documentation into the tool. In addition, the Project Hosts ISSO will perform testing of all of the application level controls and handle completion of the implementation plan and SLCM inside of eMASS on the mission partners behalf.
  - Project Hosts will provide mission partners with a FedRAMP authorized document repository dedicated to them to manage all documentation which allows for collaboration between the teams in an efficient and secure manner.
- Outside of the A&A Process, Project hosts is your dedicated Security team. The Project Hosts team provides your typical PaaS services along with many services outside of the normal PaaS offering taking most of the sustainment / continuous monitoring burden out of the mission partners hands so they can focus on their actual mission.
  These services include:
  - Managing Access Control and Authentication
  - Implementing and monitoring Azure Network Security Groups (firewall Rules) around all subnets dedicated to the mission partner
  - Auditing/ reviewing audit logs and alerts
  - Monitoring systems for availablity and performance issues/ proactively taking action
  - Monthly Operation System, Database, Web application vulnerability scanning using approved ACAS scanner
  - Monthly STIG compliance scanning
  - Patch and vulnerabiltiy management
  - Configuration Management
  - Malware prevention and Intrusion prevention using HBSS Tools
  - Dedicated Incident Response and Analysis Team
  - Contingency and Disaster Recovery Planning and recovery team
  - Managed 3PAO Scanning and Penetration Testing of the Application
  - Provides Monthly Application level POA&Ms to the mission partner for review

- Impact Level 5 Onboarding Services
  - Project Hosts recognizes that the onboarding process can look daunting upon first glance but our mission is to make it as easy on you as possible. We will dedicate a team to your onboarding efforts to assist in any way possible whether it be through the RMF process or simply filling out a document. The Project Hosts security compliance team is here for you. Throughout the rest of this document are steps required for the mission partner to be onboarded to the environment which Project Hosts will assist and advise you on.

OVERVIEW OF REQUIREMENTS

At a high level there are 7 actions that must be performed in order for you to connect to the Project Hosts FPCDoD and be fully operational at impact level 5. Each of these are broken down into more detail in the following sections.

- Provide a CSSP who will perform certain functions that a DoD component is required to do
- Complete a DoD Cloud IT Project Initial Contact form
- Register your application in SNAP and wait for approval
- After approval for registration, complete all the required fields and provide necessary artifacts with Project Hosts assistance.
- Obtain a Cloud Permission to Connect from DISA
- DISA enables access to your application through the BCAP
- Perform Continuous Monitoring.

PREREQUISITES AND OTHER CONSIDERATIONS:

The SNAP Registration process requires you to submit a lot of different registration numbers which Project Hosts can't perform for your C-ITP. Project Hosts can provide you with the information you need for these registrations and work for you to complete them but they should be started at the beginning of the Project to ensure there are no roadblocks in engaging with the DISA CAP team. In addition, eMASS or your RMF tool often require these for the A&A process.

These registrations include:

DITPR https://ditpr.dod.mil
DADMS (If NAVY to include USMC)
SNAP-IT
eMASS
PPSM https://pnp.cert.smil.mil/
Account Creation on DISA Storefront https://disa-storefront.disa.mil/

The RMF Process should also be worked in tandem with deep dive discussions to ensure it is completed and an ATO is granted in a timely manner to submit with the SNAP package for DISA's review.

REQUIREMENT 1: PROVIDE A DOD APPROVED CSSP

Each mission partner should begin this engagement with the CSSP in parallel to the RMF Process to ensure the alignment is ready to go when the ATO is granted and the CAP connection process is started. Project Hosts Recommends C5ISR as the CSSP Provider as they are already aligned with Project Hosts and understands the business relationship between PH and our Mission Partner Customers.

The CSSP must be able to perform the activities in the table below that are not handled by Project Hosts. This is mandated by Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings memorandum dated November 15, 2017. More detail about the Activities listed below is provided in that memo:

https://rmf.org/wp-content/uploads/2018/05/DoD-CIO-Memo-CS-Activities-Perf-for-Cloud-Serv-Activ-Offerings.pdf

Project Hosts FPCDoD in support of *"Mission Partner Application"*	
Cybersecurity Activity	**Responsible Party**
Vulnerability Assessment and Analysis (VAA)	
• External Vulnerability Scans	*Project Hosts*
• Web Vulnerability Scans	*Project Hosts*
External Assessment (Choose 1)	
• DoD Cyber Red Team Operations • Non-DoD Red Team • Penetration Testing • Intrusion Assessment	*(PenTest) Project Hosts 3PAO*
Vulnerability Management	
• Apply DoD required security configurations	*Project Hosts*
• Perform actions to mitigate potential vulnerabilities or threats	*Project Hosts*
• Monitor Vulnerability Management Compliance	*Project Hosts*
• Report Vulnerability Management Compliance	*CSSP*
Malware Protection	
• Malware Protection Implementation	*Project Hosts*
• Malware Notification	*CSSP*
Information Security Continuous Monitoring (CM)	
• Maintain continuous visibility into endpoint devices	*Project Hosts*
• Correlate asset and vulnerability data with threat data	*CSSP*
Cyber Incident Handling	
• Network Security Monitoring/Intrusion Detection for Boundary Cyberspace Protection (BCP)	*CSSP*
• Network and Endpoint Security Monitoring at the Enclave Level	
• Incident Reporting	*Project Hosts*
• Incident Response – Analysis	
• Incident Handling Response	*CSSP*

	Project Hosts *Project Hosts*
DODIN User Activity Monitoring (UAM) for DoD Insider Threat Program • Employ UAM capabilities to detect anomalous insider activity • Maintain insider threat audit data • Correlate insider threat audit data with Counter Intelligence	*Project Hosts* *Project Hosts* *CSSP*
Warning Intelligence and Attack Sensing and Warning (AS&W) • AS&W for BCP • AS&W at the application • Warning Intelligence	*CSSP* *CSSP* *CSSP*
Mission Owner Support and Cybersecurity Training	*Project Hosts*
Information Operation Condition (INFOCON) & Orders (e.g. TASKORD, OPORD, FRAGO, etc.) Compliance/Network Operations (NETOPS) Awareness • INFOCON & Orders Implementation • INFOCON & Orders Notification and Assistance	*CSSP* *CSSP*

REQUIREMENT 2: COMPLETED A DOD CLOUD IT PROJECT INITIAL CONTACT FORM

This Document can be found in the Box.com Repository provided by Project Hosts in the initial registration folder/ Templates titled "DoD C-ITP Initial Contact Form" It can also be accessed here: https://disa.deps.mil/ext/CloudServicesSupport/Cloud%20Form%20Repository/Forms/AllItems.aspx

Project Hosts can help you complete this form. When completed it should be digitally signed by POC who completed it and emailed to disa.meade.re.mbx.disa-commerical-cloud@mail.mil. Please CC josh.krueger@projecthosts.com and scottc@projecthosts.com in this communication

REQUIREMENT 3: REGISTER YOUR C-ITP IN THE SNAP DATABASE (NIPR ONLY)

The SNAP registration is the core requirement for initiating the connection to the DISA BCAP and receiving the Cloud Authority to Connect from the DISA BCAP. This registration and maintenance of the registration can only be performed on the NIPRNet.

1. Proceed to https://snap.dod.mil
    1. Scroll to bottom of homepage and select request a snap Account.
    2. Download and Complete the DD Form 2875 (available on the reference Documents webpage) Fill out section 13 by specifying the DISA SNAP and user role for your CC/S/A Federal agency and request access to the:
        1. Mission Owner C-ITP Module
        2. VPN Module (if required)
        3. NIPR Module (if required)
        4. Non-DISN Connections Module
2. Complete your profile data (asterisk indicate required fields)
3. Click “Submit Request: for approval”
4. DISA CAO will review submission and contact you within three business days through email on whether the account was approved or denied.

REQUIREMENT 4: UPDATE SNAP DATABASE WITH PERTINENT REQUIRED INFORMATION

The SNAP registration is the core requirement for initiating the connection to the DISA BCAP and receiving the Cloud Authority to Connect from the DISA BCAP. This registration and maintenance of the registration can only be performed on the NIPRNet. Please review this section Carefully as the Mission partner has several registrations they must perform on their side prior to having the proper information to submit on this page. These can be seen in the prerequisite section above. If Project Hosts is in parentheses below then we can provide you with the required information for submission.

1. Login to snap using credentials provided when your account was approved
2. Navigate to the Cloud Mission Owner Module (C-ITP) and provide all of the information and documentation below:

   ☐Business Case Analysis https://dodcioext.osd.mil look for Enterprise IT BCA Attachment under "Hot Items"
   ☐ATO
   ☐DoD PA (Project Hosts)
   ☐FedRAMP ID (Project Hosts)
   ☐Information Impact Level (Project Hosts)
   ☐Cloud Service Model (Project Hosts)
   ☐Cloud Deployment Model (Project Hosts)
   ☐PPSM registration Number must register at: https://pnp.cert.smil.mil/. (Project Hosts can provide you with a list of required ports for operation)
   ☐Whitelist Registration Number: The NIPRNet DMZ Whitelist is on SIPRNet at: https://niprdmzwhitelist.csd.disa.smil.mil/whitelist.aspx (Project Hosts)
   ☐VPN Routing and Forwarding ID (Optional)
   ☐CCSD Number (Optional)
   ☐DISA CSSO Verification
   ☐DoD C-ITP Initial Contact Form
   ☐Topology Diagram (Project Hosts)
   ☐DoD Cloud IT Project Name (Should match SNaP-IT and DITPR)
   ☐DoD C-IPT POC
   ☐Consent to Monitor (Template in box.com repository)
   ☐DITPR Number https://ditpr.dod.mil
   ☐SNAP-IT Number
   ☐PROJECT HOSTS FPCDOD Name/Title
   ☐CSSP SLA
   ☐Contract Number
   ☐IP Addresses For all unclassified connections (More information in section 5)

Once all of the required fields are filled in you can submit the package by selecting submit at the bottom of the screen.

REQUIREMENT 5: DISA ISSUES A CLOUD PERMISSION TO CONNECT

This will only be performed after the following requirements are met.

1. Order Connection to DISA BCAP. This can be done on the DISA Direct Store Front https://disa-storefront.disa.mil/dsf/logon?a=DDR&r=https%3A%2F%2Fddsf.disadirect.disa.mil%2Fkinetic%2FDisplayPage%3Fname%3DDDSF_Home
2. Obtained IP Space

The NIC has allocated IP address space for the PJHFPCDoD. You can request this IP Space by following the below steps. (Please consult with Project Hosts to see if this is necessary)

a. Log into https://www.nic.mil.

b. Select "Whois Search."

c. Type in: CLOUD*.

d. Under the column labeled "Network Name" use the handle ORG-NAV-PHI-1 and NIC-140-17-32-1

e. Enter in all of the required information and submit for approval. Please work with Project Hosts team to accomplish this.

REQUIREMENT 6: DISA ENABLES ACCESS TO YOUR APPLICATION THROUGH THE BCAP

Once the Registration Process in Snap is Completed the DISA Cloud Program Management Office will work in parallel with the team issuing the Cloud Permission to engineer the connection with the FPCDoD.

The goal of this is to activate the connection when DISA issues the CPTC for your application.

REQUIREMENT 7: PERFORM CONTINUOUS MONITORING

A. Comply with, Maintain and update the ATO.

   Mission owners must continuously monitor compliance with conditions set forth in section 5.3.1.2 of the DoD Cloud Computing SRG. They must also submit timely renewal request prior to the expiration date when specified in the ATO or CPTC.

B. Meet all contract requirements including those specified in DFAS
C. Must maintain awareness of USCYBERCOM OPORDS and directives issued via SIPRnet and have personnel cleared for access to OPORDS that may be classified and ensure the C-ITP complies with application US CYBERCOM OPORDS
D. Fulfill Cyber Security Service Requirements

   Ensure the PROJECT HOSTS FPCDOD is complying with the requirements in accordance with the DoD Cloud SRG and annual re-assessment requirements.

E. Conduct Continuous monitoring and incident response

   DoD requires an ongoing assessment and authorization capability which builds upon the DoD RMF and the foundation of the FedRAMP continuous monitoring strategy. These ongoing assessments include continuous monitoring and change control. It also includes aligning with a CSSP and reporting cyber incidents in accordance with normal DoD processes using the Joint Incident Management System.

F. Comply with USCYBERCOM Disconnect Orders

   Non-Compliance or cyber incidents may result in USCYBERCOM to order DISA to disconnect temporarily the service from the DISN until either the C-ITP or PROJECT HOSTS FPCDOD comply with the connection requirements.

G. Maintain the DISA Snap account

   SNAP users must annually submit their certificate of completion for the DoD Annual Cybersecurity Awareness Training to DISA connection approval office for their accounts to remain active.

H. Maintain accurate information in SNAP. The Mission owner must ensure the information about the C-ITP in DISA SNAP is updated to reflect the current accurate and complete status of the C-ITP including personnel contact information.

TASK COMPLETION TRACKER

Priority Items:

Have you registered the C-ITP in?

☐DITPR: Enter DITPR Number here: _____

☐SNAP: Enter the SNAP ID here:_____

☐DADMS (If applicable): Enter DADMS ID here_____

☐SNAP-IT: Enter SNAP-IT Number here: _____

☐eMASS: Enter eMASS Number here: _____

☐PPSM: Enter PPSM Number Here:_____

☐Created account on DISA StoreFront?

☐Issued an ATO for the C-ITP and finished validation of RMF

Completed Requirements:

☐Requirement one: Align with a CSSP

☐Requirement two: Completed and emailed DoD CITP Initial Contact Form

☐Requirement three: Register your C-ITP in the SNAP Database

☐Requirement four: Update SNAP Data Base with Required documentation and submitted to DISA

☐Requirement five: Received Cloud Permission to Connect

☐Requirement six: DISA allows connection through BCAP

REFERENCE DOCUMENTATION AND TEMPLATES:

Project Hosts has extracted and provided for you relevant Security documentation and all of the templates needed for completion in your box.com repository.

- Including your C-ITP Specific Security Package Documentation and templates for Mission Partner Customer responsibility controls.
- Relevant Templates for submission including the C-ITP Initial Contact Form, PPSM Template, Consent to Monitor template etc.
- Dataflow and Architecture Diagrams
- DISA Guideline DOCS to Include the Cloud Computing SRG, DISN CPG and Cloud Connection Process guide, DoD Instruction 8401.01 (Internet Domain Name, IP Address Space Use and Approval Guidance) and the Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings memorandum dated November 15, 2017
- Penetration test and Application Scan Results