Data Center Services Inc

Connecting Impact Level 4\5 Cloud Environments

to the

DoD Information Network (DoDIN)

Course Description

A critical component of the Impact Level (IL) 4\5 cloud migration strategy in the DoD environment is to securely connect mission owner systems to the DoD Information Network (DoDIN) via a DISA managed Cloud Access Point (CAP). This process begins with the creation of a Cloud Information Technology Project (C-ITP) on the DISA Systems/Network Approval Process (SNAP) portal and culminates with the actual network connection from the Cloud Service Provider (CSP) to the DoDIN. Prior to the physical connection, the mission owner will receive an Official DISA Cloud Permission to Connect (CPTC) document and will need to schedule a "connection deep dive" session with the DISA SCCA Team to walk through the connection process. A core component of the connection process is the activation of the cloud network advertisement and the activation of the NIPRNet routing. During this connection process the mission owner will configure the connection and immediately begin testing the NIPRNet network connectivity.

The overall end-to-end CAP connection process can become very complicated, burdensome, and can take an extended amount of time if not managed efficiently. Key issues that complicate the connection to an Army network are the Joint Regional Security Stack (JRSS) implementation at the location submitting the CAP request, authentication and application protocols transiting DISA boundaries, security infrastructure components such as HBSS and ACAS, and testing routing as implemented via the DISA default routes.

This course is designed to prepare the individuals who will be responsible for managing, requesting, or implementing CAP connection process and overcome the obstacles routinely experienced during the process. It is based on direct experience with the DISA Secure Cloud Computing Architecture (SCCA) team, Cloud Service Providers, and the actual implementation and maintenance of active CAP connections.

Data Center Services Inc

Course Syllabus

Day 1

Introduction to the DoD Cloud Environment

DoD Off-Premises

DoD On-Premises

Information Impact Levels:

- Information Impact Level 2
- Impact Level 2 Location and Separation Requirements
- Information Impact Level 4
- Impact Level 4 Location and Separation Requirements
- Information Impact Level 5
- Impact Level 5 Location and Separation Requirements
- Information Impact Level 6
- Impact Level 6 Location and Separation Requirements

Cloud Access Point (CAP)

- Internal CAPs (ICAPs)
- Boundary CAP (BCAP)
  - DISA Enterprise BCAP
  - DoD Component BCAP (e.g., the Navy BCAP)
  - NIPRNet BCAP Meet-Me Points

DISA Systems/Network Approval Process (SNAP)

- The Cloud Information Technology Project (C-ITP) Registration and Connection
- Complete a DoD C-ITP Initial Contact Form
- Determine Initial C-ITP Prioritization for Connection to a CSP-CSO
- Complete Registration of the C-ITP in DISA SNAP
- Connect the C-ITP to an Authorized CSP-CSO Via an Appropriate Gateway
- On-board the C-ITP to an Authorized CSP-CSO
- C-ITP Connection Sustainment and Maintenance Process

Day 2

Introduction to Secure Cloud Computing Architecture

- Overview
- DoD Cloud Security Guidance
- Networks and Topology
- Cybersecurity Capabilities
- Architecture Roles and Responsibilities

Introduction to Joint Regional Security Stack (JRSS)

- Overview
  - Installation Service Nodes (ISN)
  - Special Purpose Processing Nodes (SPPN)
- Multiprotocol Label Switching (MPLS)
- Virtual Routing and Forwarding (VRF)
- Impact of JRSS MPLS on Army Network Connectivity

Day 3

Ports and Protocols

- Overview
- Category Assurance List (CAL)
- Ports, Protocols, and Services Management (PPSM) Registry
- Ports, Protocols, and Services (PPS) Request
- Methodologies for Analyzing PPS Requests

The SNAP Request Package

- Process Overview
- Required Documentation
- Template Diagrams

Day 4

Building the SNAP Package

- Requirements Review
- Authentication
  - End Users
  - System Administrators
- Network Connectivity
  - End Users
  - System Administrators
- SCCA Compliance Review
  - Virtual Data Center Security Stack (VDSS)
  - Virtual Data Center Manage Services (VDMS)
  - Trusted Cloud Credential Management (TCCM)
- Ports and Protocols Review
- Network Topology Review

Supporting Documentation Review

Day 5

Implementing and Monitoring CAP connections

- Organizational CAP vs System level CAP
- Implementing CAP connections
  - Azure
  - AWS

Additional Requirements

Who Should Attend

- Anyone working in or transitioning to a DoD IL 4\5 cloud environment
- Anyone who wants to understand the principles and concepts of the DoD cloud environments and connectivity
- Developers
- Cloud architects
- System administrators
- Cyber security architects
- Cloud Security Control Assessors – Validator (SCA-V) not familiar with DoD cloud environments

Prerequisites

- A basic understanding of Microsoft Azure and Amazon AWS cloud environments
- Familiarity with the DISA Secure Cloud Computing Architecture (SCCA)
- Familiarity with DISA Cloud Security Requirements Guide (SRG)
- Ability to understand basic cloud service concepts
- Familiarity with Microsoft Visio

Hands-on Exercises

To reinforce the concepts discussed in the course, hands on guided exercises complete with solutions are provided. The exercises take the student step by step through the implementation of a CAP request and implementation for both Microsoft Azure and Amazon AWS cloud environments

What You Will Receive

- A USB drive containing all reference material and SNAP request document templates
- Course books
- A course exercise workbook with solutions

About the Author

Robert Hermanns is a principal partner with DCS, a small DOD consulting and cloud services re-seller based in Portsmouth, Virginia. Robert has over 30 years of experience in large scale data center environments including AT&T, Federal Reserve, Capital One, and the DoD. He holds a MS in Telecommunications Software Technology, from Rochester Institute of Technology and a Graduate Certificate in Information Assurance, from George Mason University. Robert started as an independent consultant with the US Army in June 2005 and moved to DCS in 2007 where he remains today.

Robert specializes in multiplatform systems architectural design, cost analysis, and technical project implementation and has successfully worked on multiple US Army DoD Impact Level (IL) 4\5 cloud migrations.

4517 Glencove Drive, Portsmouth, Virginia 23703