101.1

Introduction to the DoD Cloud Environment

www.d8acenter.com

DCLD 101 | DoD Cloud Access Point Implementation

Introduction to the DoD Cloud Environment

This page intentionally left blank

DoD Cloud Strategy Overview

Business and mission dependence on IT created

- Larger complex IT infrastructures
- Larger complex IT infrastructures became more inefficient and costly
- Average time to deliver DoD IT programs 91 months[1]
- Some new IT programs become outdated before full implementation

DoD strategic plan

- Use commoditize IT functions
- Transform IT
  - Acquisition
  - Operations
  - Management

DoD Cloud Strategy Overview

DoD strategic plan implemented in 4 concurrent steps[2]

1. Foster adoption of cloud computing
2. Optimize data center consolidation
3. Establish the DoD enterprise cloud environment
4. Deliver cloud services

DoD Cloud Strategy Overview

Foster adoption of cloud computing[3]

- Establish joint governance
- Adopt “Cloud First” approach when delivering IT systems
- Reform IT financial, acquisition, and contracting
- Implement awareness campaign
  a) Gather input from major stakeholders
  b) Expand consumer base
  c) Expand provider base
  d) Increase visibility of available cloud services through out DoD

Optimize data center consolidation[4]

- Establish joint governance

DoD Cloud Strategy Overview

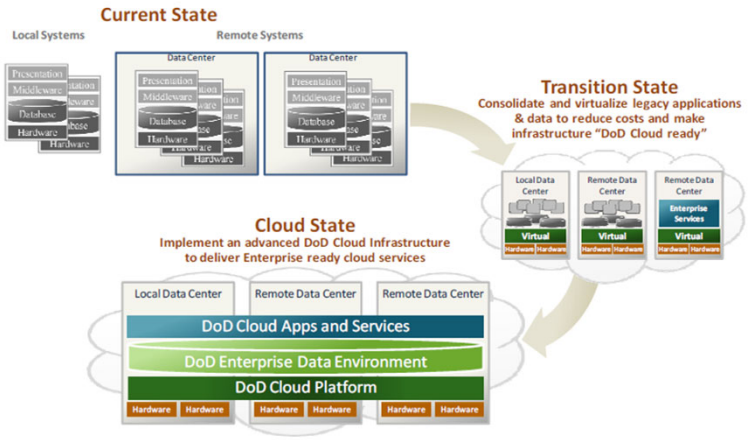
Establish the DoD enterprise cloud environment[5]

- Incorporate cloud infrastructure in data center consolidation
- Optimize delivery of multi-provider cloud services through cloud brokers
- Drive continuous service innovation using Agile methodologies
- Drive secure information sharing

Deliver cloud services[6]

- Leverage externally provided commercial cloud services
- Expand cloud services available to DoD

DoD Cloud Strategy Overview



Source: DoD ClO Cloud Computing Strategy, July 2012

DoD Cloud Strategy Overview

Cloud benefits: Efficiency, Agility, Innovation	
Efficiency	
Cloud Benefits	**Current Environment**
Improved asset utilization (server utilization > 60-70%)	Low asset utilization (server utilization < 30% typical)
Aggregated demand and accelerated system consolidation (e.g., Federal Data center Consolidation initiative)	Fragmented demand and duplicative systems
Improved productivity in application development, application management, network, and end-user devices	Difficult to manage systems
Agility	
Cloud Benefits	**Current Environment**
Purchase "as-a-Service" from trusted cloud providers	Years required to build data centers for new services
Near-instantaneous increases and reductions in capacity	Months required to increase capacity of existing services
More responsive to urgent agency needs	
Innovation	
Cloud Benefits	**Current Environment**
Shift focus from asset ownership to service	Burdened by asset management
Tap into private sector innovation	De-coupled from private sector innovation engines
Encourages entrepreneurial culture	Risk-averse culture
Better linked to emerging technologies (e.g.,	

Source: DoD ClO Cloud Computing Strategy, July 2012

DoD Cloud Strategy Overview

Transformation initiatives to improve mission effectiveness and cybersecurity

Reengineered information infrastructure

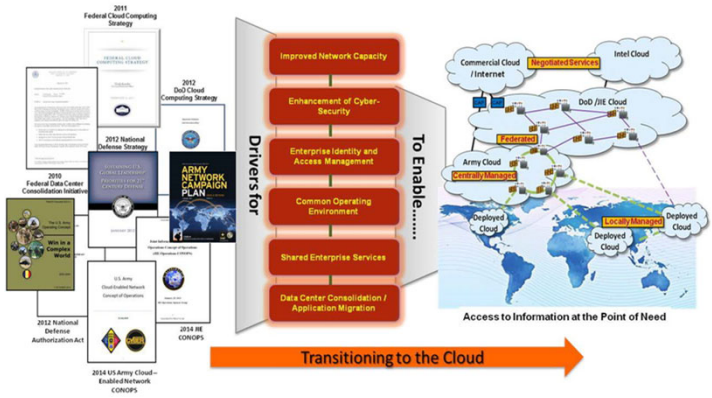
The result of this new effort is Joint Information Environment (JIE)

JIE provides

- Robust and resilient enterprise
- Delivers faster better informed collaboration and decisions
- Secure, seamless access to information regardless of computing device or location

DCS Data Center Services Inc

Army Cloud Strategy Overview



Source: Army Cloud Computing Strategy, March 2015

Army Cloud Strategy Overview

Long-term objectives

- Reduce ownership, operation, and sustainment of hardware
- Procure hardware as a service to allow Army to focus resources more effectively on the mission
- Increase operational efficiency
- Increase network security
- Improve interoperability with mission partners

Enabling the Joint Information Environment (JIE) and the Intelligence Community Information Technology Enterprise (IC ITE) for universal accessibility across DoD and the Army

Army Cloud Strategy Overview

Replicate demonstrated success with cloud computing within the private sector Technology breakthroughs that facilitate:

- Parallel processing methodologies
- Rapid software deployment cycles
- Improved virtualization allowing multiple applications to run simultaneously on shared physical resources
- Enhanced data center automation, which significantly reduces requirements for system administration labor (application of STIGs, RMF accreditation)
- Near-universal software interoperability standards

Data center consolidation combined with a cloud computing, provides utility-based model

- On-demand, pay-for-use services
- Highly competitive business opportunity

DCS Data Center Services Inc

Army Cloud Strategy Overview

Current Army IT environment is comprised of independently owned and managed

- IT infrastructure
- Systems
- Databases

Army strategic plan

- Migrate to cloud based centrally managed network
- Reduce IT hardware ownership
- Enable information sharing across domains
- Transform IT
  - Acquisition
  - Operations
  - Management

Army Cloud Strategy Overview

Cloud computing guiding principles[7]

- Common standards
- Enable resilience
- Use appropriate deployment model
- Cybersecurity cloud protection
- Lower IT costs
- Greater agility
- Service delivery under disconnected, intermittent, and low bandwidth (DIL) conditions
- Minimize redundant data sources
- Interoperability and portability
- Mission Effectiveness

Army Cloud Strategy Overview

Army Strategic Imperatives[8]

1. Adopt Cloud Governance and Management Practices
2. Instantiate Cloud Computing Capabilities within the Army Network
3. Manage the Modernization and Migration of Applications, Systems, and Data
4. Secure and Manage Cloud Operations

Army Cloud Strategy Overview

Adopt Cloud Governance and Management Practices[9]

- Synchronize planning, resourcing, and acquisition
- Develop policies and governance to monitor\enforce compliance
- Develop architectures that facilitate adoption and usage of cloud capabilities

Instantiate Cloud Computing Capabilities within the Army Network [10]

- Increase Network throughput
- Identify and leverage appropriate cloud service models
- Integrate secure mobile computing capabilities

DCS Data Center Services Inc

Army Cloud Strategy Overview

Manage the Modernization and Migration of Applications, Systems, and Data[11]

- Maintain single application migration office
- Modernize applications to conform and operate in standard environments
- Ensure data is visible, accessible, understandable, and trusted
  - Army Information Architecture

Secure and Manage Cloud Operations[12]

- Ensuring security and reducing risk
- Develop standards for acquiring and managing cloud operations

Army Cloud Strategy Overview

Army Cloud Computing Deployment Models					
On-Premise (DoD Network & Facilities)			Off-Premise (Non-DoD Federal or Commercial Facilities) * Must be within defined US Jurisdictional areas Only	Off-Premise (Non-DoD Federal or Commercial Facilities) * Must be within defined US Jurisdictional areas Only	Operationally Deployable
Gov't Owned Gov't Operated	Gov't Owned Cml Operated	Cml Owned Cml Operated	Federal Tenants Only	Multi-Tenant	Army Tactical Infrastructure
DoD Community Cloud			Federal Community Cloud	Public / Federal Community Cloud	DoD Community / Army Private Cloud
CC SRG Impact Levels up to 6			CC SRG Impact Levels up to 6	CC SRG Impact Levels up to 4	CC SRG Impact Levels 4 to 6

Source: Army Cloud Computing Strategy, March 2015

DoDI 8530.01 March 7, 2016

Identifies a set of cybersecurity activities that are required for DoDIN operations and DCO internal defensive measures to protect the DoDIN.

These activities include, but are not limited to:

- Vulnerability Assessment and Analysis
- Vulnerability Management
- Malware Protection
- Information Security Continuous Monitoring (ISCM)
- Cyber Incident Handling
- DoDIN UAM for DoD Insider Threat Program
- Warning Intelligence

DoDI 8530.01 March 7, 2016

Information Security Continuous Monitoring (ISCM)

"ISCM provides constant observation and analysis of the operational states of systems to provide decision support regarding situational awareness and deviations from expectations.

Overall ISCM furnishes ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, cyber hygiene, and cybersecurity operational readiness"[13]

DoDIN UAM for DoD Insider Threat Program

"DoDIN user monitoring capability and system auditing capability will support UAM to detect, deter, and mitigate insider threats"[14]

Warning Intelligence and Attack, Sensing, and Warning (AS&W)

"Provides the capability to receive notice of AS&W and warning intelligence information provided by intelligence organizations such as DIA and the National Security Agency"[15]

"Supports analysis of threats, suspicious or malicious network traffic, and attacks"[16]

DoDI 8530.01 March 7, 2016

DoD Cybersecurity Activities Performed for Cloud Service Offerings

Cybersecurity Activities	IaaS		PaaS		SaaS	
	Level 2	Level 4/5	Level 2	Level 4/5	Level 2	Level 4/5
Vulnerability Assessment and Analysis (VAA)						
External Vulnerability Scans	○	○	○	○	○	○
Web Vulnerability Scans	○	○	○	○	○	○
External Assessment (*An external assessment must be performed annually. The AO will select the external assessment(s) that best fit the need of the application or mission system. The AO has the option to choose all of the external assessments, but only one is required annually.)						
DoD Cyber Red Team Operations	●	●	●	●	●	●
Non-DoD Red Team	○	○	○	○	○	○
Penetration Testing	○	○	○	○	○	○
Intrusion Assessment	○	○	○	○	○	○
Vulnerability Management						
Apply DOD required security configurations	○	○	○	○	○	○
Perform actions to mitigate potential vulnerabilities or threats	○	○	○	○	○	○
Monitor Vulnerability Management Compliance	○	○	○	○	○	○
Report Vulnerability Management Compliance	●	●	●	●	●	●
Malware Protection						
Malware Protection Implementation	○	○	○	○	○	○
Malware Notification	●	●	●	●	●	●

Source: DoD CIO Cybersecurity Activities Performed for Cloud Service Offerings

DoDI 8530.01 March 7, 2016

Information Security Continuous Monitoring (ISCM)						
Maintain continuous visibility into endpoint devices	○	○	○	○	○	○
Correlate asset and vulnerability data with threat data	●	●	●	●	●	●
Cyber Incident Handling						
Network Security Monitoring/Intrusion Detection for Boundary Cyberspace Protection (BCP) Functions (as defined in ref (r))	N/A	●	N/A	●	N/A	●
Network and Endpoint Security Monitoring at the Enclave Level	○	○	○	○	○	○
Incident Reporting	●	●	●	●	●	●
Incident Response - Analysis	○	○	○	○	○	○
Incident Handling Response	○	○	○	○	○	○
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	●	●	●	●	●	●
Warning Intelligence and Attack Sensing and Warning (AS&W)						
AS&W for BCP	N/A	●	N/A	●	N/A	●
AS&W at the Application	○	○	○	○	○	○
Warning Intelligence	○	○	○	○	○	○

Source: DoD CIO Cybersecurity Activities Performed for Cloud Service Offerings

DoDI 8530.01 March 7, 2016

	Information Operations Condition (INFOCON) & Orders (e.g. TASKORD, OPORD, FRAGO, etc.) Compliance/Network Operations (NETOPS) Awareness						
	INFOCON & Orders Implementation	○	○	○	○	○	○
	INFOCON & Orders Notification and Assistance	●	●	●	●	●	●
Additional Activity	Mission Owner Support and Cybersecurity Training	○	○	○	○	○	○

●	CSSP function must be performed by a DoD CSSP or DoD CSSP entity; functions cannot be performed external to DoD hosting environments or by a commercial service provider.
○	CSSP function may be hosted and performed by a DOD CSSP, DoD CSSP entity, or can be contracted out (internal to the Component or external to a Provider). An Authorizing Official (AO) needs to consider the risk and determine who will be responsible for providing the capability/activity.
N/A	Not Applicable

Source: DoD CIO Cybersecurity Activities Performed for Cloud Service Offerings

DoD On\Off -Premises Cloud Environments

BCP - Boundary Cyberspace Protection

MCP - Mission Cyberspace Protection

ICAP - Internal Cloud Access Point

BCAP - Boundary Cloud Access Point

DoD On\Off -Premises Cloud Environments

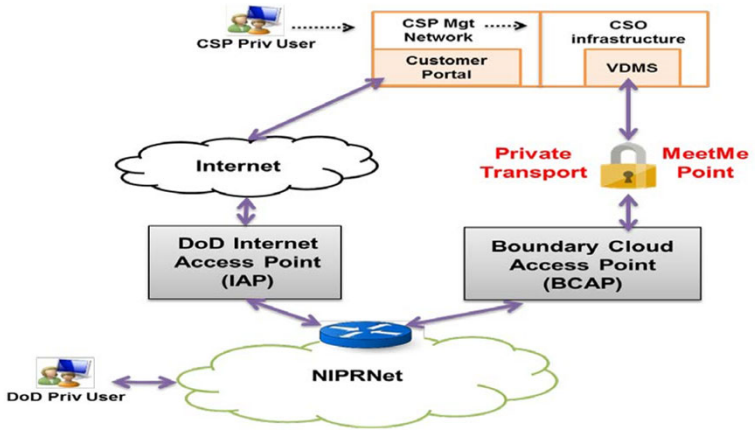
DoD Off-Premises

"A facility (building/container) or IT infrastructure is Off-Premises if it is NOT physically or virtually on DoD owned or controlled property (i.e., On-Premises)"[17]

DoD On-Premises

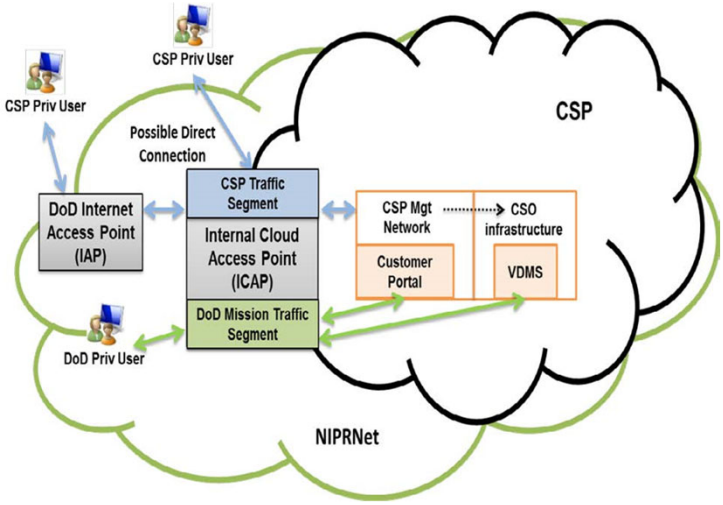
"A facility (building/container) or IT infrastructure is On-Premises if it is physically on DoD owned or controlled property. That is, it is within the protected perimeter (walls or "fence line") of a DoD installation (i.e., Base, Camp, Post, or Station (B/C/P/S) or leased commercial space) which is under the direct control of DoD personnel and DoD security policies"[18]

DoD Off -Premises Cloud Environments



DCS Data Center Services Inc

DoD On -Premises Cloud Environments



DoD On\Off -Premises Cloud Environments

On-Premises CSO Level 2/4/5 (Including milCloud):

"A mission owner utilizing a CSP on-premises must acquire through a contract or perform Mission Cyber Protection (MCP) (authorized cybersecurity service provider (CSSP)) to protect systems, applications, and/or data hosted in the cloud service model. It does not establish a dedicated connection via the BCAP or require support from an organization providing BCP. Monitoring and protection from events or incidents originating from the Internet are accomplished at the IAP or the internal cloud access point (ICAP)"

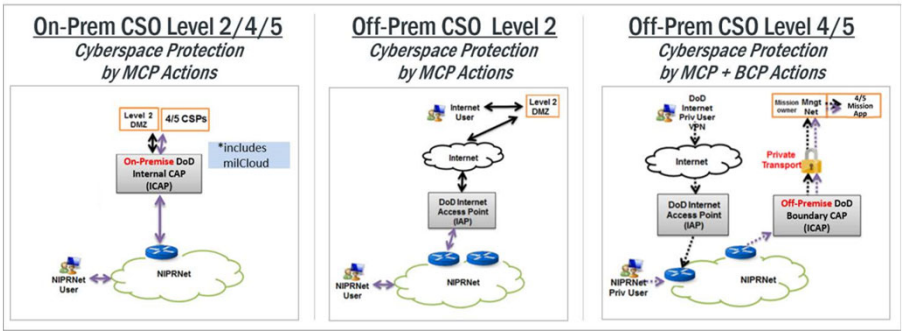
Off-Premises CSO Level 2:

"A mission Owner utilizing an off premises CSO requires support from an organization providing MCP (authorized CSSP) to protect systems, applications, and and/or data hosted in the cloud service model. For an Information Impact Level 2 CSO, the CSP off premises does not use a BCAP and does not require support from an organization providing BCP"

Off-Premises CSO Level 4/5:

"A mission owner utilizing an off premises CSO requires support from an organization providing MCP (authorized CSSP) to protect systems, applications, and/or data hosted in the Cloud. If the mission owner utilizes an off premises CSO for Information Impact Level 4/5, they must establish a dedicated connection via a BCAP. The BCAP requires support from an organization providing BCP for all connections through that BCAP"

DoD On\Off-Premises Cloud Environments



Information Impact Levels

Cloud Computing Security Requirements Guide

Version 1, Release 2

Cloud security information impact levels are defined by the combination of:

1) the sensitivity or confidentiality level of information (e.g., public, private, classified, etc.) to be stored and processed in the CSP environment; and
2) the potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information.

DoD Mission Owners must

1.) Categorize mission information systems in accordance with DoDI 8510.01 and CNSSI 1253

2.) Identify the Cloud Information Impact Level

Information Impact Levels

Impact Levels

Level 1: Unclassified Information approved for Public release

- No longer used merged with level 2

Level 2: Non-Controlled Unclassified Information

Level 3: Controlled Unclassified Information

- Level 3 is no longer used and has been merged with Level 4

Level 4: Controlled Unclassified Information

Level 5: Controlled Unclassified Information

Level 6: Classified Information up to SECRET

Information Impact Levels

Information Security Impact Levels		Definitions
CSM	CC SRG	
1		Unclassified, publicly releasable information, e.g., recruiting websites
2	2	Unclassified, publicly releasable information with access controls, e.g., library systems
3		Non-National Security System (non-NSS) Controlled Unclassified Information (CUI) – low confidentiality impact, moderate integrity impact, e.g., training systems
4	4	Non-NSS CUI – moderate confidentiality impact, moderate integrity impact, e.g., human resource systems, personally identifiable information (PII), and protected health information (PHI)
5	5	NSS CUI – moderate confidentiality impact, moderate integrity impact, e.g., email systems
6	6	Classified information up to and including Secret â€" moderate confidentiality impact, moderate integrity impact, e.g., command and control systems

Source: Army Cloud Computing Strategy, March 2015

Information Impact Levels

Level 2: Non-Controlled Unclassified Information

"Includes all data cleared for public release, as well as some DoD private unclassified information not designated as Controlled Unclassified Information (CUI) or critical mission data, but the information requires some minimal level of access control"

Level 4: Controlled Unclassified Information (CUI)

"CUI is information the Federal Government creates or possesses that a law, regulation, or Government-wide policy requires, or specifically permits, an agency to handle by means of safeguarding or dissemination controls. CUI requires protection from unauthorized disclosure"

- **Export Controlled-**--Unclassified information concerning items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives.
- **Privacy Information (PII)**
- **Protected Health Information (PHI)**
- **Other information requiring explicit CUI designation (i.e., For Official Use Only, Official Use Only, Law Enforcement Sensitive, Critical Infrastructure Information, and Sensitive Security Information)**

Information Impact Levels

Level 5: Controlled Unclassified Information

"Accommodates CUI that requires a higher level of protection than that afforded by Level 4 as deemed necessary by the information owner, public law, or other government regulations. Level 5 also supports unclassified National Security Systems (NSSs) due to the inclusion of NSS specific requirements in the FedRAMP+ C/CE"

Level 6: Classified Information up to SECRET

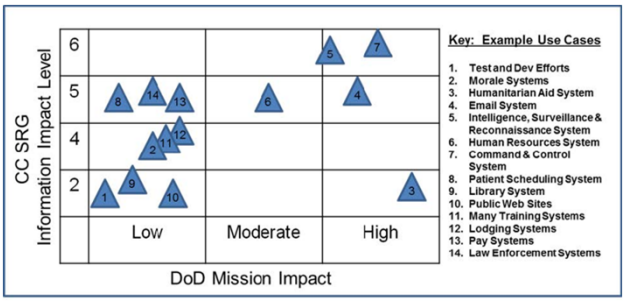
Level 6 accommodates information that has been determined to be classified national security information"

Information Impact Levels

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

DCS Data Center Services Inc

Information Impact Levels



Source: Army Cloud Computing Strategy, March 2015

Cloud Access Point (CAP)

A CAP is a system or network boundary providing protection and network monitoring capabilities

- Sometime referred to as a cybersecurity IA stack
- Primary function is to protect the Defense Information System Network (DISN)
- Secondary function is to protect DoD Information Network (DoDIN)
- Not designed to protect systems or applications (mission owner responsibility)
- All cloud based systems processing DoD sensitive data must connect users via a CAP

Cloud Access Point (CAP)

Basic capabilities of a CAP include

- Firewall capability to restrict DISN traffic
- Firewall rules deny all traffic originating via CSO IP address ranges (non-DoD)
- Provides IDS capabilities to detect firewall failures, unauthorized traffic, and malware
- Provide voice and video protection
- Provide data feeds to DoDIN cyber defense capabilities

Cloud Access Point (CAP)

Boundary CAP (BCAP)

- Sometimes referred to as “Enterprise CAP”
- Required for all “off-premises” IL4/5 commercial cloud operations
- Provides DISN perimeter defenses and cyber defenses for traffic flowing to and from CSO hosted applications
- Protects DoDIN (DoD missions within DISN) from incidents originating inside the CSP’s infrastructure
- Protects DoD systems and applications in one CSP environment from incidents in another CSP environment

Cloud Access Point (CAP)

NIPRNet BCAP

Must be implemented as a system of hyper redundant, dual homed, geographically disbursed, high availability, high capacity cybersecurity stacks and meet-me points

Not required for IL 2 environments

IL 4/5 environments all internet traffic flows through NIPRNet Internet Access Point (IAP)

Direct physical connection between DISN, meet-me router, and CSP router

Serves as authorized DMZ for Internet Facing Applications (IFA) and mission systems in IL 4/5 provided DoD IP address range is DoD DMZ authorized IP addresses

Cloud Access Point (CAP)

NIPRNet BCAP Meet-Me Points

DISN Point-of-Presence (POP) located in telecommunications carrier agnostic interconnection facility

High capacity router and may include boundary defenses

Purpose is to facilitate interconnection of DISA BCAP with multiple CSP networks

Physical fiber connection between multiple CSPs and DISA equipment in facility

Facility must meet FedRamp security requirements with isolated and secured DoD Hardware

CSP connection to interconnect facility never traverses the Internet

Cloud Access Point (CAP)

Boundary CAP (BCAP)

- Mission owner must submit DISA Systems/Network Approval Process (SNAP) Cloud Information Technology Project (CITP) request
- Each mission owner environment considered an enclave
- Mission owner systems must protect their systems
  - Implement DMZ
  - Implement Virtual Data Center Security Stack (VDSS)
  - Implement Virtual Data Center Management Suite (VDMS)

Cloud Access Point (CAP)

Internal CAP (ICAP)

- Used in commercially owned and operated on-premise cloud environment
- Provides DISN perimeter defenses and cyber defenses for traffic flowing to and from on-premises CSO hosted applications
- Protects DoDIN (DoD missions within DISN) from incidents originating inside the CSP's infrastructure
- Protects DoD systems and applications in one CSP environment from incidents in another CSP environment

DISA Systems/Network Approval Process (SNAP)

The Cloud Information Technology Project (C-ITP) Registration and Connection Process

- 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

DISA Systems/Network Approval Process (SNAP)

Review

DISA SNAP Account Registration Process Diagram

DoD Cloud Information Technology Project (C-ITP) Registration & Connection Process

DoD Cloud Access Point (CAP) Connection Provisioning Process

www.d8acenter.com

45