DEPARTMENT OF DEFENSE (DoD)
Secure Cloud Computing Architecture (SCCA)
Functional Requirements

1/31/2017
V2.9

Developed by the
Defense Information Systems Agency (DISA)
for the
Department of Defense (DoD)

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

DOCUMENT INFORMATION

CHANGE / REVISION RECORD	
Date	Description of Change
01/16/2015	Initial functional requirements description
02/02/2015	Update on functional requirements document
02/09/2015	Updates to address results of 2/7/15 review with DISA leadership
2/13/2015	Updates to address results of 2/10/15 review with DISA leadership and MITRE Team Review
3/17/2015	Updates to address comments
4/2/2015	Update to address RE comments
4/10/2015	Update to address RE & CTO comments
4/22/2015	Update to address RE comments
6/15/2015	Update to address RE & CC/S/A comments
6/24/2015	Update to add network requirements
6/30/2015	Update to add CAP Extension Appendix
7/15/2015	Update to address administrative comments from PAO and removed FOUO marking.
10/30/2015	Update to address DoD community and CSP comments
2/23/2016	Renamed CAP FRD to SCCA FRD and updated to include SCCA components
10/31/2016	Update to address industry and DoD Component comments
1/31/2017	SCCA Pilot Team Inputs

Executive Summary

As the Department of Defense (DoD) strives to meet the objectives of the DoD CIO to maximize the use of commercial cloud computing, the Defense Information System Network (DISN) perimeter and DoD Information Network (DoDIN) systems must continue to be protected against cyber threats. DISA is responsible for developing the DISN protection requirements and guidance to secure the connection point to the Cloud Service Provider (CSP). DISA is well positioned to provide enterprise capabilities to secure DoD Mission Owner systems deployed to the commercial cloud.

The purpose of the Secure Cloud Computing Architecture (SCCA) is to provide a barrier of protection between the DISN and commercial cloud services used by the DoD while optimizing the cost-performance trade in cyber security. The SCCA will proactively and reactively provide a layer of overall protection against attacks upon the DISN infrastructure and mission applications operating within the commercial cloud. It specifically addresses attacks originating from mission applications that reside within the Cloud Service Environment (CSE) upon both the DISN infrastructure and neighboring tenants in a multi-tenant environment. It provides a consistent CSP independent level of security that enables the use of commercially available Cloud Service Offerings (CSO) for hosting DoD mission applications operating at all DoD Information System Impact Levels (i.e. 2, 4, 5, & 6).

Requirements defined herein cover the array of CSOs to include Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). However, the authors have been careful to word requirements with sufficient specificity to address the DoD cloud security posture while enabling innovation and allowing flexibility in implementations. The shared responsibility model is assumed to persist so that, where important for cost savings, identified security capabilities can be delivered by either DoD, commercial CSP, or 3rd party organizations.

1 Introduction

The DoD has made great strides in protecting the DoD Information System Network (DISN) from security threats at its boundary through Non-secure Internet Protocol Router Network (NIPRNet) hardening initiatives. As the DoD move to maximize the use of commercial cloud computing, the DISN perimeter must continue to be protected against cyber threats from external connections. As such, DISA is responsible for developing the requirements to support the DoD in implementing DISN perimeter protection at the connection point to multiple Cloud Service Providers (CSP). DISA is also well positioned to provide enterprise protection capabilities for mission applications and Mission Owner (MO) data hosted within the commercial Cloud Service Environment (CSE).

This document provides a summary of the Secure Cloud Computing Architecture (SCCA) and its requirements based upon and analysis of possible attack vectors. The boundary requirements that were developed apply to all cloud service offerings including: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). SCCA requirements have been developed based upon the DoD experiences covering successful implementations of commercial and other non-DoD systems. Such systems have included Internet Access Points (IAPs), NIPRNet Federated Gateway (NFG), and direct connections to approved contractor facilities. SCCA requirements are intended to be consistent with Joint Information Environment (JIE) objectives[1].

1.1 Scope

This document addresses functional requirements necessary to enable detection, protection, and response to cyber security threats against the DISN from Non-DoD on- or off-premise CSPs. It also provides functional requirements for the protection, detection, and response to cyber security threats against DoD systems deployed into commercial CSEs for all DoD Information System Impact Levels (i.e., 2, 4, 5, & 6). The requirements currently specified within this document pertain only to the security and associated interoperability necessary to facilitate secure deployment and operations of DoD IT systems incorporating commercially owned cloud based Information Technology (IT) services.

The SCCA provides a capability and governance model, which is built upon guidance and requirements provided by the DoD Cloud Computing Security Requirements Guide (SRG)[2]. As such, it is based upon the handling of systems and information categorized by all DoD mission Impact levels.

1.1.1 DISN Boundary Security

The SCCA is designed to meet the boundary protection needs of the DISN by protecting the DISN from cyber-attacks originating from within the CSP's CSE. A CSE may be comprised of an array of CSOs from a particular CSP; wherein, a CSO is one or a bundle of cloud services offered for sale by the CSP. Implementing the SCCA will mitigate potential damages to the DISN and will provide the ability to detect and prevent an attack before reaching the DISN. It will provide a consistent level of security that facilitates the implementation of commercial provided cloud services to support DoD mission applications.

[1] DoD Cybersecurity RA

[2] DoD CC SRG

1.1.2 DoD Cloud Hosted System Security

The SCCA establishes the capabilities and governance models through which to protect DoD mission owner enclaves, application servers, virtual systems, and information hosted within the commercial cloud. Functional requirements defined herein are applicable for all CSO environments (i.e., IaaS, PaaS, SaaS). However, use of the SCCA is not a mandate. It is recognized that commercial CSPs, 3rd Party Providers, and DoD Mission Owners may deliver DoD compliant security solutions with the approval of the assigned Authorization Official (AO).

1.1.3 Cloud Governance

The SCCA addresses the need for specialized DoD governance over IT systems and operations that employ commercial CSOs. While existing DoD data center STIGs and emerging JIE requirements apply, the SCCA specifically addresses the need to tightly control privileged user access (including root) to the commercial CSP's CSO management and configuration systems. Unlike typical on-premise DoD data centers, these systems are generally accessible from the internet or other non-DoD controlled communication networks. Additionally, these systems employ the CSP's Identity and Access Management (IdAM) systems which may not be federated with an authorized DoD IdAM system. While the governance model typically applies well for IaaS and some PaaS offerings, it may not apply to SaaS and some PaaS offerings where cloud consumers are excluded from CSO administration systems. The SCCA privileged cloud user access governance model applies specifically to the use of access control systems provided and managed by the CSP.

1.1.4 Implementation Guidance

SCCA functional requirements are intended to provide DoD-wide capabilities for the secure implementation and employment of commercial CSOs. This document does not specify the DoD Organization responsible to deliver or operate SCCA technical components. However, DISA is responsible for protection of the DISN and will therefore provide for enterprise boundary defense and associated DISN connection services. While DISA will develop and deliver SCCA enterprise services, DoD Components and Mission Owner elements may develop and deliver their own SCCA technical components in accordance with requirements specified herein. However, DISA's SCCA enterprise services are intended to reduce the cost of deployment and operations of DoD cloud hosted systems. It is generally expected that SCCA technical components implemented by one DoD organization could be made available to other DoD organizations and mission partners. Accordingly, capability and operational consistency across technical component implementations is desired.

1.2 Secure Cloud Computing Architecture Technical Components and Topology

The SCCA is specifically architected and intended to deliver the security capabilities defined by the DoD Cloud Computing Requirements Guide (CC SRG) as necessary to support secure deployment of DoD systems and information into the commercially owned and operated CSP industry segment. A DoD Provisional Authorization (PA) provides a validation of a CSP's compliance with the DoD CC SRG guidance for hosting systems operating at an indicated DoD System Impact Level. Assuming a CSP has achieved a DoD PA, the SCCA defines DoD system implementation and governance requirements necessary to protect the DISN boundary and commercial cloud hosted DoD mission systems and information; illustrated in Figure 1. The construction of the SCCA is intended to levy no additional requirements upon the commercial CSP industry other than those related to secure connectivity.

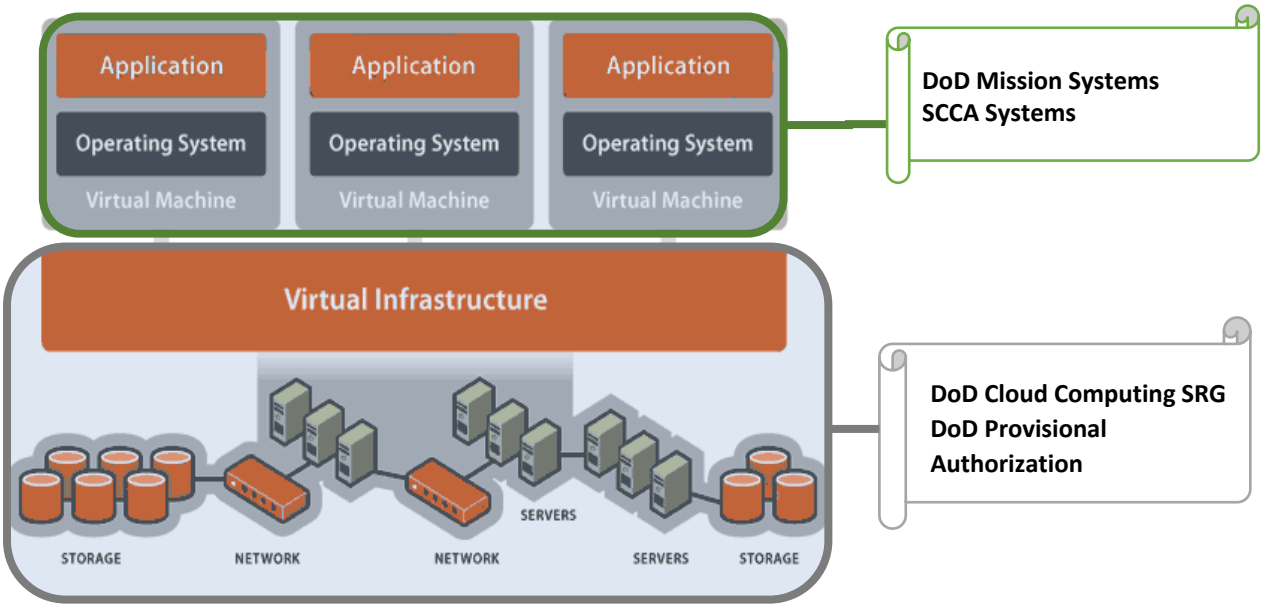


Figure 1. Cloud Computing Foundations

The SCCA is broken into four technical components to allow flexible implementation and DoD IT organization ownership. As illustrated in

Figure 2, it is comprised of:

- Cloud Access Point (CAP):
  The CAP provides access to the Cloud, boundary protection of DISN from the Cloud, and cyber defense capabilities such as firewall and intrusion detection and prevention (IDS/IPS) at the DISN boundary. Full packet capture (FPC) and interface translation may be provided, as needed, to support secure connectivity and access to individual commercial cloud hosting systems. The CAP is specifically tailored to operate at DoD Impact levels 4 and 5. In order to support both on-premise and off-premise Non-DoD CSPs, CAP requirements are decomposed into Internal-CAP (ICAP) and Boundary-CAP (BCAP) requirements.
- Virtual Datacenter Security Stack (VDSS):
  The VDSS provides DoD Core Data Center (CDC)-like network security capabilities such as firewall, intrusion detection, and intrusion prevention systems. It also provides application security capabilities such as web application firewall (WAF) and proxy systems. The VDSS can reside within or outside of the CSP's infrastructure (virtually or physically). VDSS capabilities can also be provided as-a-Service by a third party vendor (for IaaS) or a CSP (for IaaS and SaaS). VDSS feeds should be provided to a DoD Cybersecurity Service Provider (CSSP) performing enclave boundary defense. The VDSS also supports sharing of security event data among cyber security stakeholders. The VDSS is specifically tailored to operate at all DoD Information Impact Levels.

- Virtual Datacenter Managed Services (VDMS):
  The VDMS provides system management network and mission owner system support services necessary to achieve JIE management plane connectivity and mission owner system compliance. It provides secure management network connectivity to the DISN, virtual host based management services, and identity and access management services for DoD Controlled Access Card (CAC) authentication to virtual systems. The VDMS is specifically tailored to operate at all DoD mission Impact Levels. VDMS functionality applies directly to IaaS environments but may not be specifically applicable to PaaS and SaaS CSOs as such functionality may be inherent to the associated CSP and validated through the DoD PA
- Trusted Cloud Credential Manager (TCCM):
  The TCCM is an individual or entity appointed by the DoD mission owner's Authorizing Official (AO) to establish plans and policies for the control of privileged user access (to include root account credentials) used to establish, configure, and control a mission owner's Virtual Private Cloud (VPC) configuration once connected to the DISN. The TCCM establishes and manages Least-Privilege Attribute-Based Access Control (ABAC) accounts and credentials used by privileged DoD users and systems to administer and control DoD CSO configurations. The role of TCCM is intended to operate at all DoD information Impact Levels. However, the TCCM may not apply to some SaaS solutions where DoD account owners are not required to use the CSP's Identity and Access Management (IdAM) system to administer user accounts and service configurations.

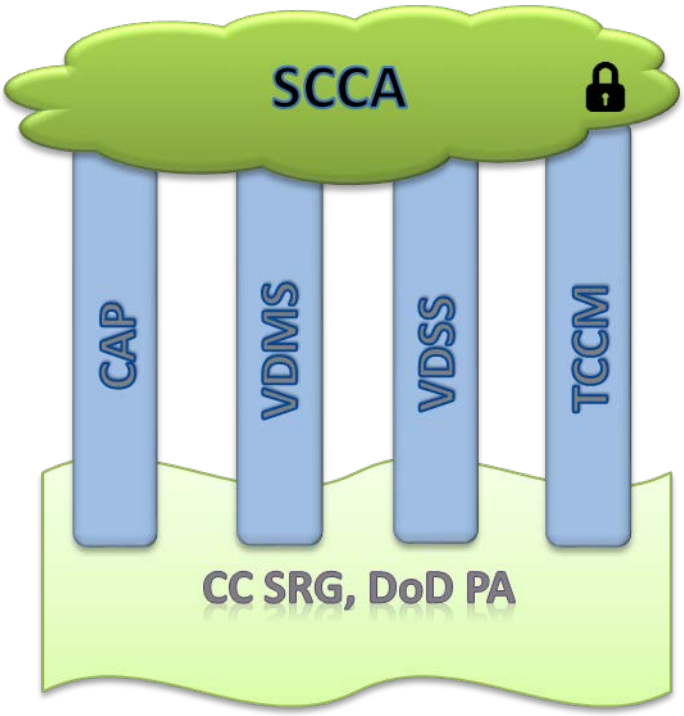


Figure 2. Secure Cloud Computing Architecture (SCCA) Components

With the exception of the TCCM, SCCA component functional requirements are considered applicable to all cloud service models (i.e., IaaS, PaaS, and SaaS). However, requirements are not specific to provider. SCCA technical capabilities may be delivered by the responsible DoD organization, a DoD authorized CSP, or an authorized 3rd party Security-as-a-Service (Sec-aaS) provider. Users of the SCCA are intended to be responsible DoD Mission Owners or DoD Components accredited as a CSSPs by USSTRATCOM IAW DoD O-8530.01-M. For typical IaaS and PaaS solutions, all CAP, VDSS, VDMS, and TCCM requirements are considered applicable. However, for some SaaS solutions, VDSS and VDMS functionality may be delivered by the CSP and authorized under the DoD Provisional Authorization (PA). For CSOs where DoD consumers are not given privileged user access control and management capabilities, the TCCM is not applicable.

1.2.1 DoD Cloud Security Guidance

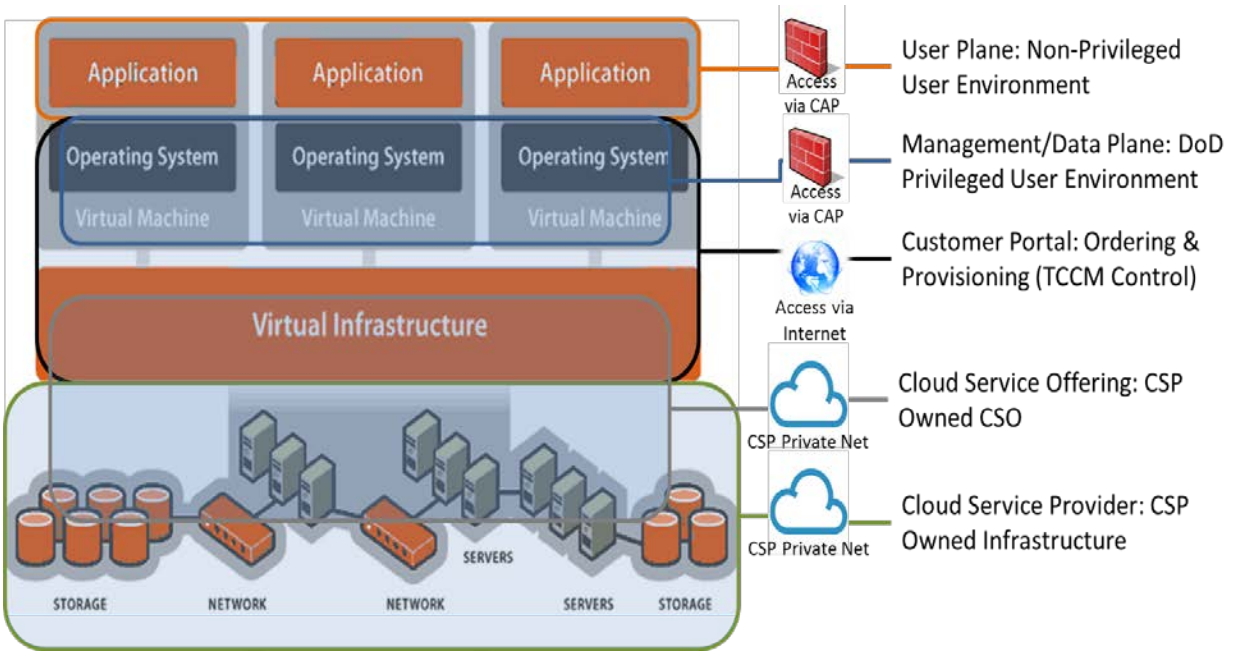
In accordance with the DoD Cloud Computing SRG, DoD cloud access systems will enable CSP connections to the DISN consistent with security objectives identified by the information impact levels described therein. The SRG provides guidance for the implementation of cloud access systems[3]. An Internal CAP (ICAP) allows connectivity between the DISN and a non-DoD (US Commercial) "On-Premise" CSP such as milCloud 2.0. JIE requirements and DoD Data Center architectures govern security capabilities for "On-Premise" CSP connectivity and to the DISN.[4] The Boundary CAP (BCAP) allows connectivity between the DISN and a non-DoD (US Commercial) "Off-Premise" CSP.

1.2.2 Networks and Topology

There are several networks in use when hosting a DoD mission application within a CSP as illustrated by Figure 3. There are the CSP's private networks that are used by the CSP to manage the underlying infrastructure and CSO implementation, such as the physical host systems, network infrastructure, the virtualization layer, and service hosts. Access to these networks is limited to authorized CSP privileged user staff and are isolated from the Internet.

[3] DoD CC SRG

[4] JIE CDC EDS



User Plane: Non-Privileged User Environment
The User Plane is the network plane where user and data traffic flow.

Management/Data Plane: Privileged-User Environment
The Management Plane carries DoD privileged users (e.g. BCND, MCND, System Administrators), maintenance, and monitoring traffic.

Customer Portal: Ordering & Provisioning
The Customer Portal is the interface where the TCCM and Mission Owner access to provision accounts, instantiate systems and/or applications, and monitor user activity.

Cloud Service Offering: CSP Owned Private Network
The CSP Owned CSO is the network plane where the various CSOs reside, including the customer portal, SaaS, and CSP-provided capabilities to support IaaS/PaaS environments (e.g. identity management, domain services).

Cloud Service Provider: CSP Infrastructure Private Network
The CSP Owned Infrastructure is the network plane where physical hosts of CSOs reside. Access to this network is out of band and is only accessible by the CSP.

Figure 3. Notional Cloud Service Provider Infrastructure & Networks

The DoD User, Data, and Management networks are virtually isolated from the CSP's private networks. The Management Plan is established inside the CSE virtual network layer and provides Mission Owner (MO) administrators and security operations personnel access to MO virtual systems. The Data Plane is a network used for back-end communications between applications system tiers. The Production Plane establishes the user environment. Each of these is virtually segmented from the others. Access to these networks is via the CAP. As such, these networks appear to a DoD user as an extension of the DoDIN.

For typical IaaS and PaaS offerings, the Customer Portal is used by CSO account holders to provision CSP services and deploy mission owner systems into the CSE (this may not be the case with SaaS offerings). CSO accounts are generated by the CSP and associated credentials are created by the CSP's DoD authorized IdAM system. The CSP's IdAM system is also be used to establish credentials and for interacting with Application Program Interface (API) and Command Line Interface (CLI) services. These systems and services are not assumed to be federated with DoD IdAM systems. Customer Portals and API/CLI service end-points are typically internet accessible. As a result, the TCCM establishes and manages the CSP originated authentication and authorization credentials for DoD users having CSO account privileges. The TCCM may employ functions of the VDMS to accomplish this role.

The DISN management network (illustrated in Figure 4) is used to manage DoD Systems and perform CND service provider operations in accordance with JIE JMN design[5]. The DISN management network and the mission owner management network will be integrated to facilitate DoD privileged user access to mission owner virtualized systems. The CAP will support connections to the mission owner management networks.[6]

The CAP will provide direct dedicated and secure network connectivity to the CSP as well as isolation for all traffic planes: User/Data, and Management. These planes may translate into Subnets, Zones or Virtual Routing & Forwarding (VRF) segments within the CSE. Within the CSE of the CSP, traffic separation will be achieved using the CSP's networking services.

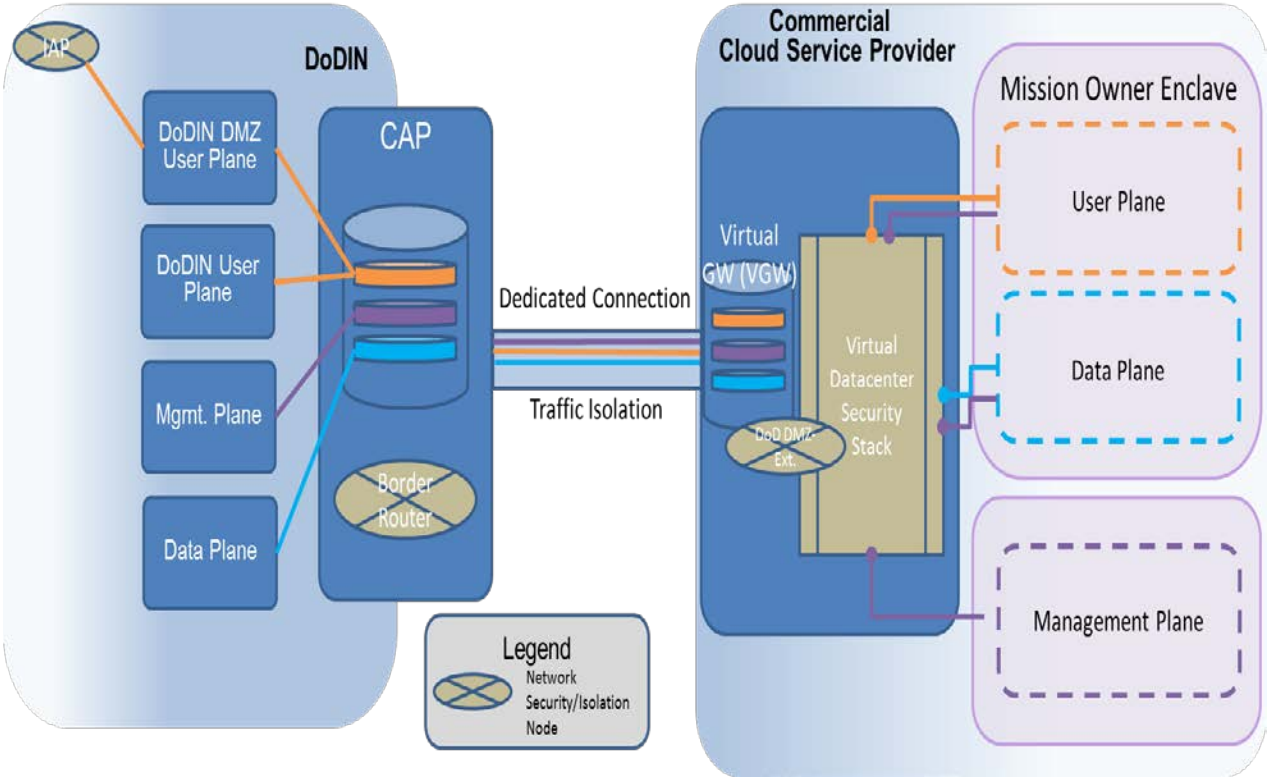


Figure 4. Notional DISN Management Networks

[5] DoD JMN EDS

[6] DoD CC SRG

1.2.3 Cybersecurity Capabilities

The SCCA provides an array of cyberspace defensive capabilities to provide DISN boundary defense and protect DoD systems and information deployed to a Commercial CSP. It has been designed to extend the DISN common security posture into the authorized commercial CSP segment while leveraging and interoperating with the broader DoD cyber security defenses. Its design achieves the DoD requirements for traffic inspection[7] and cyber security[8] while minimizing communication bandwidth demand and duplication of defenses.

1.2.4 Roles and Responsibilities

The SCCA is architected to support three (3) primary roles and responsibilities for which entity definition is provided within the DoD Cloud Computing SRG:

- Mission Owner (MO)
  A MO is a DoD entity responsible for delivering and operating a DoD mission system. MOs are responsible for the procurement, deployment, and secure operations of their mission systems deployed to the cloud environment. Accordingly, MOs are expected to maintain trusted configuration baselines and to perform continuous monitoring for deployed mission systems. Capabilities by the VDMS have been specifically selected to support this operational requirement. Additionally, the MO is required to establish or assign an entity to fulfill the requirements of the TCCM.
- Mission Cyberspace Protection (MCP)
  The MCP organization is the DoD entity charged with the responsibility of securing a MO's enclave and networked systems by establishing and delivering cybersecurity capabilities. The MCP is specifically responsible for cyber defense of MO systems. The security capabilities of the VDSS have been specifically selected to support this operational requirement. The MCP can also be the MO themselves or a certified CSSP providing MCP capabilities.
- DISN Boundary Cyberspace Protection (BCP)
  The DISN BCP organization is the DoD entity charged with the responsibility to establish and deliver cybersecurity capabilities to protect the DISN. This entity will be DISA. It is assumed that DISA will deliver CAP systems and services.

The alignment of SCCA components to cybersecurity mission is illustrated in Figure 5. Cyber security information from the CAP supports the mission of the organization providing BCD. However, cyber security information from the VDSS supports the missions of organizations providing both BCD and MCD. The VDMS acts similarly to support the missions of organizations providing both MCD and Missions. Establishment and execution of TCCM governance activities is specifically a MO responsibility.

[7] NDAA 2015
[8] DoDI 8530.01

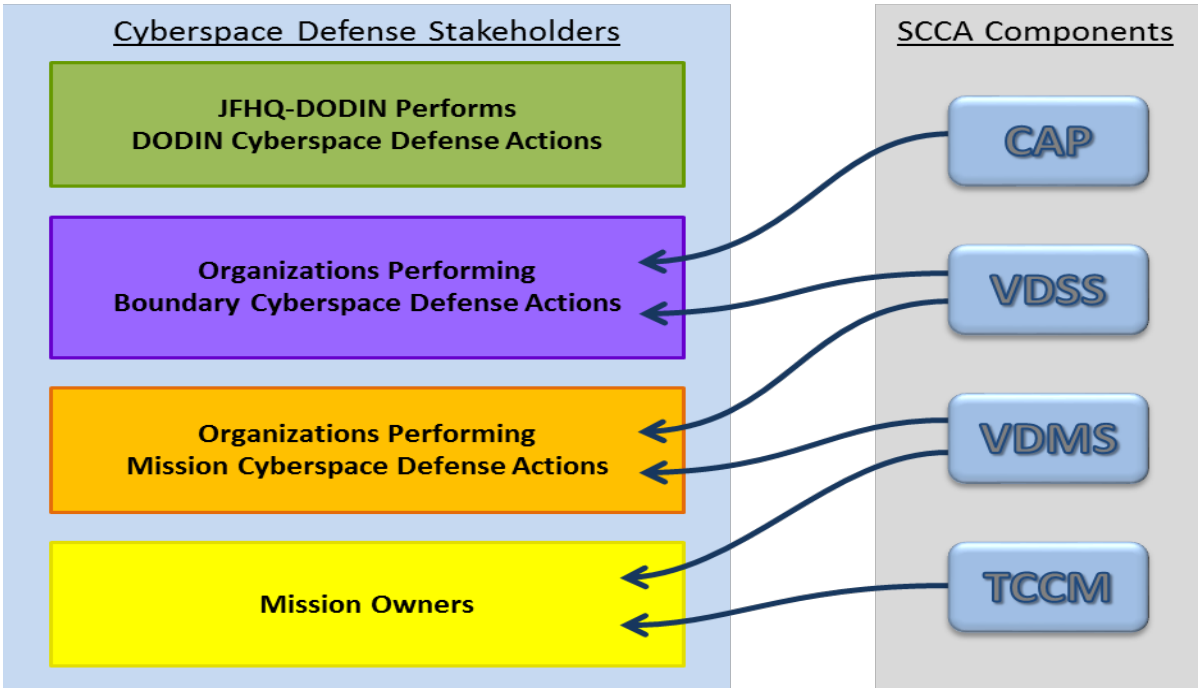


Figure 5. SCCA Component Alignment to Cybersecurity Organizations

1.2.5 Capability Modularity, Decoupling and Applicability

The SCCA security capabilities are considered modular and decoupled components. However, regardless of the owner or operator of the capability, each SCCA function is required for a comprehensive cyberspace defense capability. Additionally, individual requirements need not be specifically achieved within a given component if they can be achieved at some other point in the cybersecurity architecture. Therefore, if requirements can be met by non-SCCA systems, it is not necessary to deploy redundant systems to achieve SCCA component capabilities. For this reason, it may be possible to employ security systems and services of the CSP or other DoD systems to meet SCCA component capability requirements.

Furthermore, specification is not made regarding the division of virtual versus physical system implementation of SCCA component capabilities. As a result, SCCA components may be implemented as either physical or virtual systems. This allows for the virtualization and colocation of SCCA component systems.

Moreover, the SCCA is built upon the assumption of DoD cybersecurity information sharing. This implies that sensor data derived from SCCA component is sharable among cybersecurity service provider organizations to achieve the DoD cybersecurity mission. For example, event data derived from a Web Application Firewall (WAF), performing Secure Socket Layer/Transport Layer Security (SSL/TLS) traffic break and inspect, could be retrieved and employed by both the BCD and MCD organizations to accomplish their respective cybersecurity missions.

The SCCA is established to provide a set of components to assist DoD Mission Owners in achieving the requirements of the DoD Cloud Computing SRG. As illustrated in Figure 6, SCCA component capabilities

apply to both DoD on-premise (e.g. milCloud 2.0) and off-premise CSP systems as well as IaaS, PaaS, and SaaS CSOs operating at all Impact Levels.

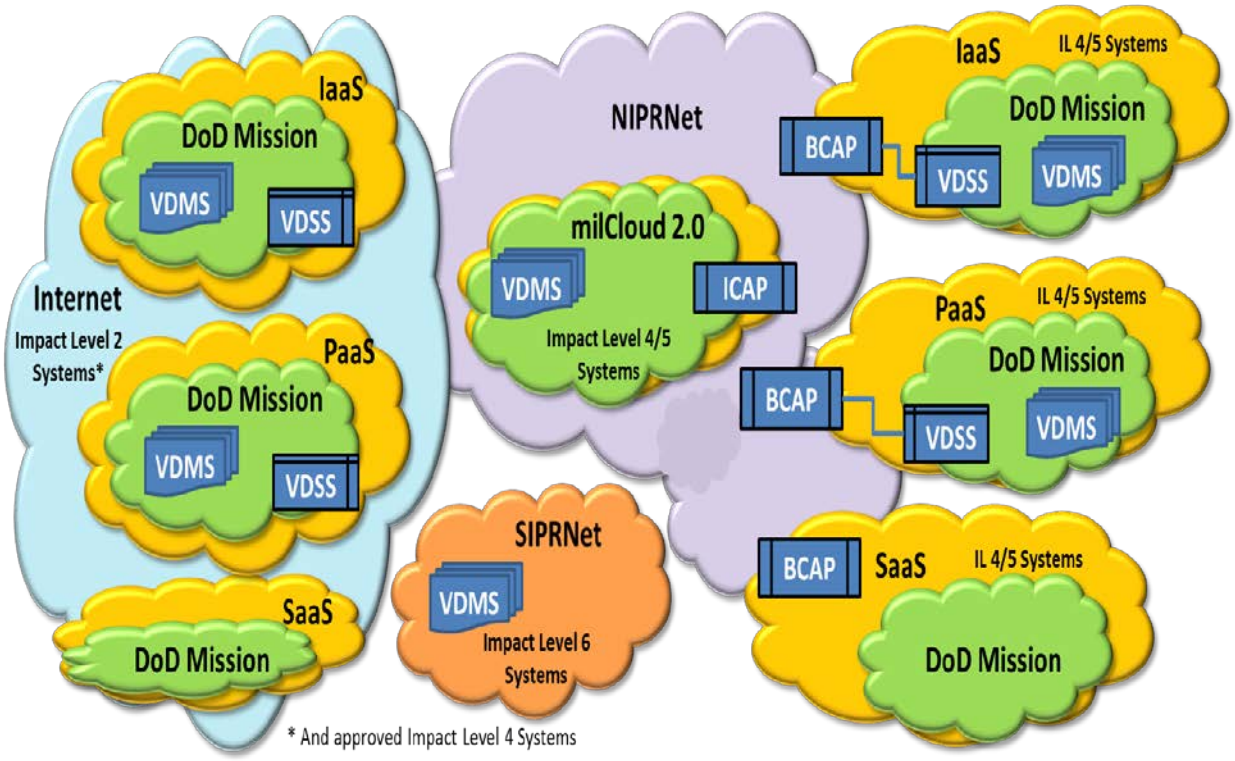


Figure 6. SCCA Component Applicability

1.3 Applicable Security Policies

Security and risk management policies applicable to any IT system deployed in a DoD environment are pertinent to the SCCA. In addition, the SCCA must comply with all privacy and Health Insurance Portability and Accountability Act (HIPAA) laws and regulations if traffic involves any personal or medical information. Guiding DoD policies are:

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D Defense Information Systems Network (DISN) Responsibilities, 4 August 2015

Committee on National Security Systems Instruction (CNSSI) 1253 Security Categorization and Control Selection for National Security Systems, 15 Mar 2012

DoD Cloud Way Forward, V 1.0; 23 Jul 2014

DoD Cloud Computing Security Requirements Guide (CC SRG), Version 1, Release 2; 18 Mar 2016.

DoD CIO Memo, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 Dec 2014

DoD OSD Memo: Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs; 1 Aug 2014

DoDI 5000.02 Operation of the Defense Acquisition System, 7 Jan 2015

DoDI 5000.44 Protection of Mission Functions to Archive Trusted Systems and Networks (TSN), 5 Nov 2012

DoDI 8500.01 Cybersecurity, 14 Mar 2014

DoDI 8550.01 Internet Services and Internet-Based Capabilities; 11 Sep 2012.

DoD Instruction 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT), dated 12 March 2014

DHS Trusted Internet Connections (TIC) Reference Architecture Document Version 2.0 Federal Interagency Technical Reference Architectures, 1 Oct 2013

National Defense Authorization Action (NDAA), 2015

NIST SP 500-292 Cloud Computing Reference Architecture, Sep 2011

NIST SP 500-293 US Government Cloud Computing Technology Roadmap Volume I, Oct 2014

NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, Apr 2013

NIST SP 800-160 Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Second Public Draft, May 2016

1.4 Reference Documents

Technical reference materials used for the creation of this document is as follows:

DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework RMF) into the System Acquisition Lifecycle, 26 May 2015

DoD Cloud Industry Day, Roger Greenwell & Peter Dinsmore; 29 Jan 2015

DoD Cybersecurity Reference Architecture, V4.0, dated 17 June 2016

DoD Security Architecture Reference Model (SARM) Description, V 3.0 (Final); 24 Sep 2014.

DoD JIE) Core Data Center (CDC) Engineering Design specification (EDS), Version 2.0; 15 Dec 2014

DoD Joint Information Environment (JIE) Enterprise Operations Center (EOC) Engineering Design Specification (EDS), Version 3.0: 13 August 2015

DoD Joint Information Management Network (JMN) Engineering Design Specification, v3.6 (draft), 30 June 2016

DoD Unified Capabilities Requirements 2013 (UCR 2013); Jan 2013

DoD Internet-NIPRNet DMZ Inc. 1, Phase 2, Technology Overview, v3, Release 1; 6 Jul 2015

DoD Enterprise Cloud Service Broker Cloud Security Model, V 2.1; 13 Mar 2014

DoDI 8551.01, Ports, Protocols, and Services Management (PPSM); 28May 2014

DoDI 8530.01 Cybersecurity Activities Support to DoD Information Network Operations, 7 March 2016

DISA NIPRNet DOD DMZ Policy Requirements Version, V 2 Release; 08 Aug 2014

DISA Network Services Telecommunications Service Level Agreement (SLA); 12 Mar 2014

DISA Network Services Virtual Private Network (VPN) Customer Ordering Guidance, V 2.4; 12 Mar 2013

DISA NIPR Federated Gateway (NFG) Network Design, V 1.4 (Draft); 12 Nov 2012

DISA Enclave Checklist V4, Release 5; 27 July 2012

DISA Secure Remote Computing Security Technical Implementation Guide (STIG) V2, Release 5; 29 July 2011

DISA Remote Access Policy Security Technical Implementation Guide (STIG) V2 Release 11; 22 Apr 2016

2 Functional Requirements

Requirements decompose into security, connectivity, and specific capabilities, such as full packet capture and integration with management system. The requirements describe the capabilities required for the SCCA to protect the DISN, establish connectivity between the DISN and the CSO, operational aspects (e.g., Disaster Recovery Plan), component management, and mission cyber defense. The SCCA requirements are a logical representation of various component capabilities.

In order to identify the security requirements, the requirements analysis process considered possible threats against the DISN from a malicious attacker on a compromised CSO virtual infrastructure component or hosted mission application. Threats were then assessed for their applicability to attacks against DISN assets. Once a threat was shown to be possible, a requirement to detect and protect was written. Further requirements were derived from the threat analysis to address the data handling requirements necessary to provide effective cyber security response. Table 1 identifies the initial threats considered for derivation of SCCA security requirements. The NIPRNet/SIPRNet Cyber Security Architecture Review (NSCSAR) Joint Task Force (JTF) will further refine and assess cyber threats to DoD cloud assets.

The following assumptions are made with respect to the threat environment for a Non-DoD CSP Cloud Service Environment (CSE):

- CSE networks and systems are owned and operated by the commercial CSP
- The CSO holds a DoD Provisional Authorization (PA) for Impact Levels 2, 4 and/or 5 in accordance with the SRG
- The CSO is accessible from the Internet for impact level 2 applications
- The CSO is only accessible from the NIPRNet via a CAP for impact level 4/5 applications
- The CSO is only accessible from the SIPRNet for impact level 6 applications
- CSP management personnel have controlled access to physical, hypervisor, and virtual environment layers

Table 1. Initial SCCA Threat Considerations

Threat Source	Information Systems Threat[9]
CSP	Virtual Machine (VM) Escape[10]
CSP	Cross VM Attack
CSP	CSP Resource Denial of Service
CSP	Session Hijack/Man-In-The Middle
CSP	Service Account Hijack
CSP	Virtual Machine Hijack
CSP	Unauthorized Virtual Machine Management Console Access
CSP	Data Exfiltration
CSP	Advanced Persistent Threat
CSP/Perimeter	Malicious Code/Malware
CSP/Perimeter	SQL Injection
CSP/Perimeter	VoIP Call Eavesdropping
CSP/Perimeter	VoIP Call Modification
CSP/Perimeter	VoIP Call Hijacking
Perimeter	VoIP System DOS
Perimeter	Network Enumeration
Perimeter	Botnet Denial of Service
Perimeter	Unauthorized IP Source/Destination
Perimeter	Virtual Local Area Network (VLAN) Hopping
Perimeter	DNS Hijacking (CSE hosted application DNS request)
Perimeter	IP Route Hijacking
Perimeter	IP Address Spoofing
Perimeter	Rogue Access Device/Access Point Hijack (com carrier traffic interception or adding to IaaS Local Area Network (LAN))

[9] Appendix B: Threat Definitions

[10] Virtualization layer threats are not assumed to exist for CSPs employing not virtualized hosting environments

Threat Source	Information Systems Threat[9]
Perimeter	Unauthorized CAP Privileged User Account Access

2.1 Security Requirements

Below are the security requirements allocated to each of the SCCA components. They are judiciously selected to achieve the following objectives:

1. DISN Boundary Defense (CAP)
2. Mission Owner Enclave and Application Defense (VDSS)
3. Mission Application End-Point Defense (VDMS)
4. DISN and Mission Defense (TCCM)

The following assumptions are made with respect to implementation of a CAP solution:

- System requirements for the implementation of the DoD Enterprise Recursive Service (ERS) to support Domain Name Service (DNS) Resolution are addressed, as needed, by the ERS Program Office; associated requirements are not the responsibility of the SCCA system.
- DISN network routing to support specific and Mission Owner connectivity is addressed, as needed, by DISA Network Operations and Network Engineering Offices; associated requirements are not the responsibility of the SCCA system.
- Network requirements to enable Cloud service operations in the event of Internet Access Point (IAP) cutoff are address, as needed, by DISA Network Operations/Engineering and the individual CSP.
- Identity Federation requirements to enable CAC authentication of non-privileged DoD users to cloud hosted DoD (e.g., IaaS and PaaS) or SaaS provided systems and services is the responsibility of the CSO procuring DoD Component or Program Office; associated requirements are not the responsibility of the SCCA system.

2.1.1 Cloud Access Point

Below is a list of requirements derived from the threat risk analysis. These requirements define threat mitigation capabilities necessary to protect the DISN. As threats evolve, the CAP security requirements will also evolve to deliver risk-based defense capabilities. CAP security requirements are not specific to physical location nor logical-physical implementation. This means that the option to locate the CAP within a Cloud Service Environment (CSE) is allowed. Further, the ability to collocate the CAP with other components of the SCCA to leverage infrastructure and system sharing is permitted. CAP requirements are composed of BCAP and ICAP requirements.

2.1.1.1 Boundary Cloud Access Point

Table 2 provides BCAP security requirements. The main purpose of the BCAP is to protect the DISN. It serves as a point defense to detect and prevent intrusion, unauthorized routes, known malicious code, and malicious network activity. It security event capture data is intended for use by JFHQ-DoDIN Situational Awareness (SA) systems.

Table 2. BCAP Security Requirements

Req. ID	BCAP Security Requirements
2.1.1.1.1	The BCAP shall provide the capability to detect and prevent malicious code injection into the DISN originating from the CSE
2.1.1.1.2	The BCAP shall provide the capability to detect and thwart single and multiple node DOS attacks
2.1.1.1.3	The BCAP shall provide the ability to perform detection and prevention of traffic flow having unauthorized source and destination IP addresses, protocols, and Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) ports
2.1.1.1.4	The BCAP shall provide the capability to detect and prevent IP Address Spoofing and IP Route Hijacking
2.1.1.1.5	The BCAP shall provide the capability to prevent device identity policy infringement (prevent rogue device access)
2.1.1.1.6	The BCAP shall provide the capability to detect and prevent passive and active network enumeration scanning originating from within the CSE
2.1.1.1.7	The BCAP shall provide the capability to detect and prevent unauthorized data exfiltration from the DISN to an end-point inside CSE
2.1.1.1.8	The BCAP and/or BCAP Management System shall provide the capability to sense, correlate, and warn on advanced persistent threats
2.1.1.1.9	The BCAP shall provide the capability to detect custom traffic and activity signatures
2.1.1.1.10	The BCAP shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide control for BCND providers
2.1.1.1.11	The BCAP shall provide full packet capture (FPC) for traversing communications
2.1.1.1.12	The BCAP shall provide network packet flow metrics and statistics for all traversing communications
2.1.1.1.13	The BCAP shall provide the capability to detect and prevent application session hijacking

2.1.1.2 Internal Cloud Access Point

Table 3 provides ICAP security requirements. The ICAP provides a combination of DISN boundary protection and Mission Owner enclave protection similar to what would be expected within a Core Data Center (CDC). As such, its' requirements set is larger than that of the BCAP. From a security perspective, the ICAP must additionally protect against the possible internet backdoor connection that may be present within an on-premise commercial cloud service implementation.

The following assumption with respect to ICAP security requirements are made:

- Existing and planned CDC security systems are capable of delivering ICAP security functionality
- ICAP requirements can be achieved by deployment of any combination of physical and/or virtual systems.

Table 3. ICAP Security Requirements

Req. ID	ICAP Security Requirements
2.1.1.2.1	The ICAP shall provide the capability to detect and prevent malicious code injection into the DISN originating from the CSE
2.1.1.2.2	The ICAP shall provide the capability to detect and thwart single and multiple node DOS attacks
2.1.1.2.3	The ICAP shall provide the ability to perform detection and prevention of traffic flow having unauthorized source and destination IP addresses, protocols, and Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) ports
2.1.1.2.4	The ICAP shall provide the capability to detect and prevent IP Address Spoofing and IP Route Hijacking
2.1.1.2.5	The ICAP shall provide the capability to prevent device identity policy infringement (prevent rogue device access)
2.1.1.2.6	The ICAP shall provide the capability to detect and prevent passive and active network enumeration scanning originating from within the CSE
2.1.1.2.7	The ICAP shall provide the capability to detect and prevent application session hijacking
2.1.1.2.8	The ICAP shall provide the capability to detect and prevent unauthorized data exfiltration from the DISN to an end-point inside CSE
2.1.1.2.9	The ICAP and/or ICAP Management System shall provide the capability to sense, correlate, and warn on advanced persistent threats
2.1.1.2.10	The ICAP shall provide the capability to write and detect custom traffic and activity signatures

Req. ID	ICAP Security Requirements
2.1.1.2.11	The ICAP shall provide the capability to detect and/or prevent VoIP call eavesdropping, modification, and hijacking
2.1.1.2.12	The ICAP shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide bi-directional control.
2.1.1.2.13	The ICAP shall maintain separation of all management, user, and data traffic.
2.1.1.2.14	The ICAP shall allow the use of encryption for segmentation of management traffic.
2.1.1.2.15	The ICAP shall provide a reverse proxy capability to handle service access requests from client systems
2.1.1.2.16	The ICAP shall provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content
2.1.1.2.17	The ICAP shall provide a capability that can distinguish and block unauthorized application layer traffic
2.1.1.2.18	The ICAP shall provide a capability that monitors network and system activities to detect and report malicious activities
2.1.1.2.19	The ICAP shall provide a capability that monitors network and system activities to stop or block detected malicious activity
2.1.1.2.20	The ICAP shall perform break and inspection of Secure Socket Layer (SSL)/Transport Layer Security (TLS) communication traffic supporting single and dual authentication for traffic destined to systems hosted within the CSE. Decryption of message payloads is not implied.
2.1.1.2.21	The ICAP shall provide a monitoring capability that captures log files and event data for cyberspace analysis
2.1.1.2.22	The ICAP shall provide an archiving system for common collection, storage, and access to event logs by Boundary and Mission cyberspace privileged users
2.1.1.2.23	The ICAP shall provide a FIPS-140-2 compliant encryption key management system for storage of DoD generated and assigned server private encryption key credentials for access and use by the Web Application Firewall (WAF) in the execution of SSL/TLS break and inspection of encrypted communication sessions
2.1.1.2.24	The ICAP shall provide a DoD DMZ Extension to support connection from the NIPRNet DoD DMZ COI of supported mission owners

Req. ID	ICAP Security Requirements
2.1.1.2.25	The ICAP shall provide full packet capture (FPC) for traversing communications
2.1.1.2.26	The ICAP shall provide network packet flow metrics and statistics for all traversing communications
2.1.1.2.27	The ICAP shall provide for the inspection of traffic entering and exiting the CSE.

2.1.2 Virtual Datacenter Security Stack

The Virtual Data Center Security Stack (VDSS) serves to protect Mission Owner enclaves and applications hosted in an off-premise CSO. VDSS services may be offered by a DoD Component, Mission Owner, or Enterprise Service Provider. Such services may be provisioned from application CSP, the CSP market place, or other third party authorized provider. VDSS functionality may be deployed within the CSE, the MeetMe Point, CAP, or supporting Core Data Center (CDC), as required. VDSS requirements apply to all IaaS, PaaS, and SaaS offerings of a CSP.

The VDSS will maintain the separation of communication traffic between virtual subnets operating within the user, data, and management planes of the DISN[11]. The VDSS will perform traffic inspection and filtering of traffic to provide cybersecurity for cloud resident enclaves and mission owner applications. The VDSS will support the Cyber Security Service Provider (CSSP) organizations having either Boundary or Mission Owner defense objectives. VDSS security requirements are provided in Table 4. VDSS requirements are anticipated to apply to all cloud service models including IaaS, PaaS, and SaaS. VDSS requirements are not specific as to provider and can be delivered by either the responsible DoD organization, a DoD authorized CSP, or an authorized 3rd party provider.

The following assumptions are made with respect to implementation of a VDSS solution:

- Routing within the CSP is accomplished via CSP's Software Defined Networking (SDN).
- Routing of public IP space within the DISN for the purpose of application advertisement and whitelisting is prohibited, unless specifically authorized.
- Security information and event data from the VDSS can be made available to either the DISN Boundary CSSP, the Mission owner defense objectives. For example, SSL/TLS session data could be used to support both the MO CSSP to protect the end-point system and the Boundary CSSP to protect the DISN.
- A single DoD-managed network security enclave deployed to a IaaS or PaaS CSE may support multiple Mission Owners while maintaining virtual separation between Mission Owner virtual

[11] DoD CC SRG

environments. For SaaS providers, this assumption is validated by the DoD Provisional Authorization.

Table 4. VDSS Security Requirements

Req. ID	VDSS Security Requirements
2.1.2.1	The VDSS shall maintain virtual separation of all management, user, and data traffic.
2.1.2.2	The VDSS shall allow the use of encryption for segmentation of management traffic.
2.1.2.3	The VDSS shall provide a reverse proxy capability to handle access requests from client systems
2.1.2.4	The VDSS shall provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content
2.1.2.5	The VDSS shall provide a capability that can distinguish and block unauthorized application layer traffic
2.1.2.6	The VDSS shall provide a capability that monitors network and system activities to detect and report malicious activities for traffic entering and exiting Mission Owner virtual private networks/enclaves
2.1.2.7	The VDSS shall provide a capability that monitors network and system activities to stop or block detected malicious activity
2.1.2.8	The VDSS shall inspect and filter traffic traversing between mission owner virtual private networks/enclaves.
2.1.2.9	The VDSS shall perform break and inspection of SSL/TLS communication traffic supporting single and dual authentication for traffic destined to systems hosted within the CSE[12].
2.1.2.10	The VDSS shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide control for MCD operators
2.1.2.11	The VDSS shall provide a monitoring capability that captures log files and event data for cybersecurity analysis
2.1.2.12	The VDSS shall provide or feed security information and event data to an allocated archiving system for common collection, storage, and access to event logs by privileged users performing Boundary and Mission CND activities

[12] Management of FIPS 140-2 compliance for cryptographic components deployed to virtualized systems is the responsibility of the VDSS system owner in collaboration with the CSP and applicable 3rd party vendors. Associated risks should be addressed at Authorization.

Req. ID	VDSS Security Requirements
2.1.2.13	The VDSS shall provide a FIPS-140-2 compliant encryption key management system for storage of DoD generated and assigned server private encryption key credentials for access and use by the Web Application Firewall (WAF) in the execution of SSL/TLS break and inspection of encrypted communication sessions.
2.1.2.14	The VDSS shall provide the capability to detect and identify application session hijacking
2.1.2.15	The VDSS shall provide a DoD DMZ Extension to support to support Internet Facing Applications (IFAs)
2.1.2.16	The VDSS shall provide full packet capture (FPC) or cloud service equivalent FPC capability for recording and interpreting traversing communications
2.1.2.17	The VDSS shall provide network packet flow metrics and statistics for all traversing communications
2.1.2.18	The VDSS shall provide for the inspection of traffic entering and exiting each mission owner virtual private network.

2.1.3 Virtual Datacenter Managed Service

The VDMS is the SCCA component responsible for application host security. VDMS provides the security systems that manage the security posture of the Mission Owner Enclave. VDMS will provide common DoD Core Data Center (CDC) services[13] Such as common security and utility services, as specified in Table 5. VDMS requirements are anticipated to apply to IaaS and PaaS service models. VDMS requirements are not specific as to provider and can be delivered by either the responsible DoD organization, a DoD authorized CSP, or an authorized 3rd party provider. Associated SaaS provider requirements are considered to be validated by the DoD Provisional Authorization.

Table 5: VDMS Security Requirements

Req. ID	VDMS Security Requirements
2.1.3.1	The VDMS shall provide Assured Compliance Assessment Solution (ACAS), or approved equivalent, to conduct continuous monitoring for all enclaves within the CSE
2.1.3.2	The VDMS shall provide Host Based Security System (HBSS), or approved equivalent, to manage endpoint security for all enclaves within the CSE

[13] JIE CDC STIG

Req. ID	VDMS Security Requirements
2.1.3.3	The VDMS shall provide identity services to include an Online Certificate Status Protocol (OCSP) responder for remote system DoD Common Access Card (CAC) two-factor authentication of DoD privileged users to systems instantiated within the CSE
2.1.3.4	The VDMS shall provide a configuration and update management system to serve systems and applications for all enclaves within the CSE
2.1.3.5	The VDMS shall provide logical domain services to include directory access, directory federation, Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS) for all enclaves within the CSE
2.1.3.6	The VDMS shall provide a network for managing systems and applications within the CSE that is logically separate from the user and data networks.
2.1.3.7	The VDMS shall provide a system, security, application, and user activity event logging and archiving system for common collection, storage, and access to event logs by privileged users performing BCP and MCP activities.
2.1.3.8	The VDMS shall provide for the exchange of DoD privileged user authentication and authorization attributes with the CSP's Identity and access management system to enable cloud system provisioning, deployment, and configuration
2.1.3.9	The VDMS shall implement the technical capabilities necessary to execute the mission and objectives of the TCCM role.

2.1.4 Trusted Cloud Credential Manager

The TCCM is an SCCA business role responsible for credential management with the purpose of enforcing least privilege access for privileged accounts that are established and managed using the CSP's IdAM system. VDMS systems will provide interfaces, as appropriate, to CSP IdAM system to execute the TCCM role. The TCCM is an individual or DoD organization responsible to establish plans, polices, and procures to securely manage CSP provided Customer Portal account access credentials and privileges. The TCCM retains control over the CSO root account credential and defines and issues role based access rights for lower level credential holders. Conceptually, the TCCM becomes the owner of a Mission Owner's CSO root credential prior to approval to connect to the DISN. The intent is to provide a mechanism whereby privileges necessary to configure unauthorized network connections and destroy systems and information within the CSE are limited and tightly controlled.

The TCCM is responsible for ensuring and overseeing the proper operation of the CSP's Identity and Access Management (IdAM) system when it is made available to cloud consumers. As a result, the TCCM is considered critical for most IaaS and PaaS solutions but may not be applicable to SaaS solutions which offer no CSO management capabilities. Implementation of the TCCM function is not intended to place unique identity management requirements upon the commercial CSP segment nor does it prohibit

the use of DoD-CSP federation or third party identity broker solutions to provide the intended IdAM control.

The TCCM concept is based upon an assumption that the CSP has implemented an IdAM system to control cloud customer access to the CSP provisioning and resource configuration systems which enables management over the CSO. Such systems can include the CSP's Customer Provisioning Portal (CPP), Application Program Interface (API), and Command Line Interface (CLI) service components. Fundamental, the TCCM must lock down credentials that can be used to create unauthorized networks.

The TCCM is appointed by the Authorizing Official (AO) charged with oversight of an IT system. The TCCM is the enforcer of least privileged access model, responsible for the provision and control of commercial cloud privileged user credentials. The TCCM owns and maintains the Cloud Credential Management Plan (CCMP). Prior to connection to the DISN, DISA will validate the existence of the CCMP as part of the Connection Approval Process defined in the Connection Process Guide (CPG).

While development and management of a CCMP is a requirement for connectivity to the DISN, implementation of the TCCM does not preclude implementation and use of DoD Component, CSP, or 3rd party provided identity broker solutions. Table 6 provides TCCM functional requirements.

The following assumptions regarding TCCM requirements are made:

- The VDSS will implement the technical capabilities necessary for an individual to carry out the mission and objectives of the TCCM role.

Table 6. TCCM Security Requirments

Req. ID	TCCM Security Requirements
2.1.4.1	The TCCM shall develop and maintain a Cloud Credential Management Plan (CCMP) to address the implementation of policies, plans, and procedures that will be applied to mission owner customer portal account credential management
2.1.4.2	The TCCM shall collect, audit, and archive all Customer Portal activity logs and alerts
2.1.4.3	The TCCM shall ensure activity log alerts are shared with, forwarded to, or retrievable by DoD privileged users engaged in MCP and BCP activities
2.1.4.4	The TCCM shall, as necessary for information sharing, create log repository access accounts for access to activity log data by privileged users performing both MCP and BCP activities
2.1.4.5	The TCCM shall recover and securely control customer portal account credentials prior to mission application connectivity to the DISN
2.1.4.6	The TCCM shall create, issue, and revoke, as necessary, role based access least privileged customer portal credentials to mission owner application and system administrators (i.e., DoD privileged users).

Req. ID	TCCM Security Requirements
2.1.4.7	The TCCM shall limit, to the greatest extent possible, the issuance of customer portal and other CSP service (e.g., API, CLI) end-point privileges to configure network, application, and CSO elements
2.1.4.8	The TCCM shall ensure that privileged users are not allowed to use CSP IdAM derived credentials which possess the ability to unilaterally create unauthorized network connections within the CSE, between the CSO and the CSP's private network, or to the Internet

2.2 System Connectivity Requirements

The SCCA CAP, VDSS, and VDMS components provide secure connectivity between cloud-based systems and DISN management, user, and data networks as illustrated in

ACAS: Assured Compliance Assessment Solutions
CSAAC: Cyber-Situational Awareness Analytic Cloud
ESM: Enterprise Systems Management
FW: Firewall
HBSS: Host-Based Security Services
HSM: Hardware Security Module
IA: Information Assurance
IAP: Internet Access Point
IDS: Intrusion Detection System
IPS: Intrusion Protection System
IntTrl: Interface Translation
JIA: Joint Information Assurance
LDAP: Lightweight Directory Access Protocol
OCSP: Online Certificate Status Protocol
OOB: Out-of-Band network
RCVS: Robust Certificate Validation Service
SaaS: Software-as-a-Service WAF: SRX:
VDC: Virtual Data Center
Web Application Firewall

Figure 7. Overall, the SCCA is intended to provide the cyberspace defense capabilities necessary to support DoDIN operations in accordance with DoDI 8530.01. Accordingly, it establishes networks and connectivity to support system administration, mission operations, and cyberspace defense. It provides an extension of the Out-of-Band (OOB) network used for management and cyberspace defense and for generation and collection of security event and information. Data flows to support authorized DoD Internet and NIPRNet users are also supported.

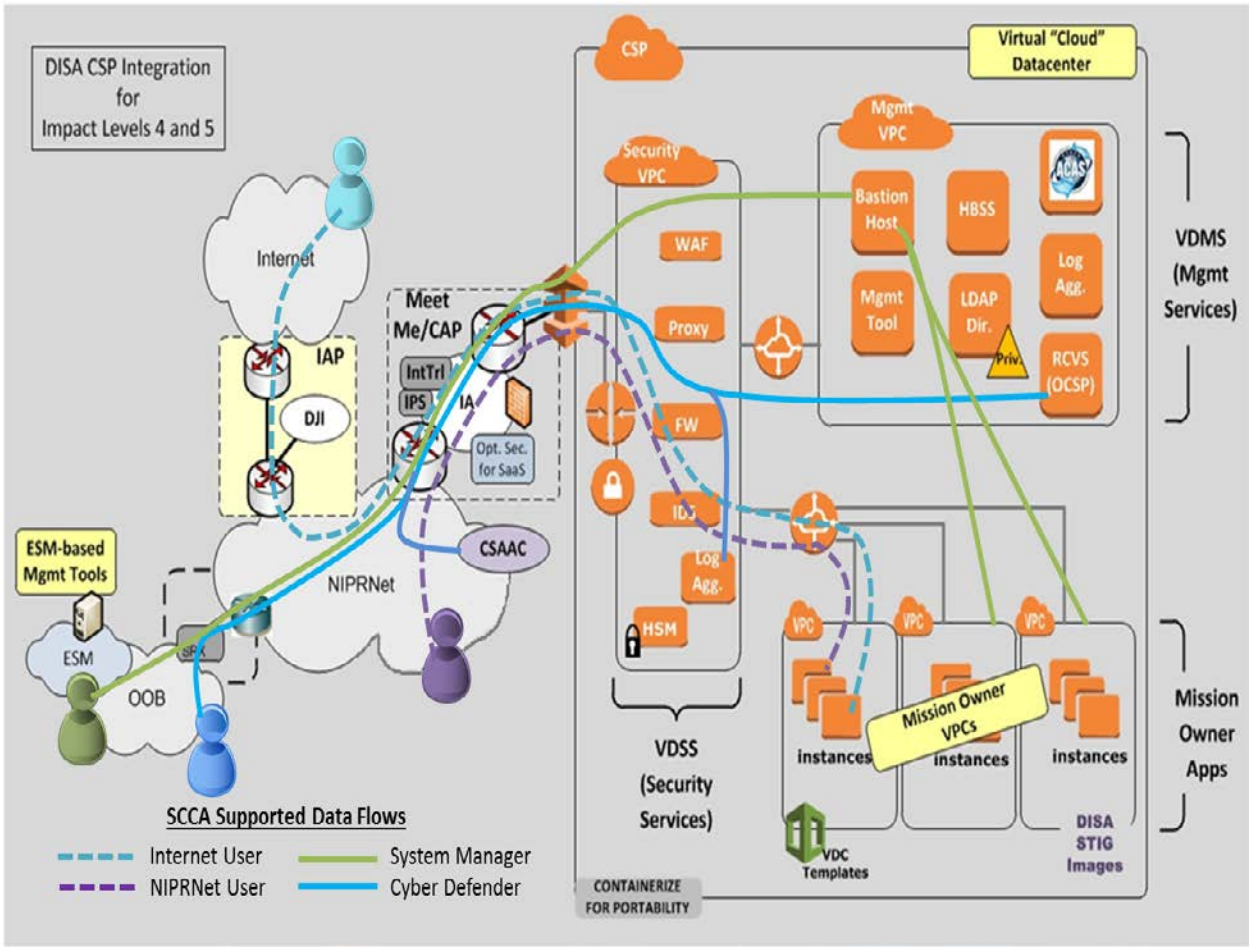
The CAP provides secure connectivity between the CSP and the DISN. Although not illustrated in

ACAS: Assured Compliance Assessment Solutions
CSAAC: Cyber-Situational Awareness Analytic Cloud
ESM: Enterprise Systems Management
FW: Firewall
HBSS: Host-Based Security Services
HSM: Hardware Security Module
IA: Information Assurance
IAP: Internet Access Point
IDS: Intrusion Detection System
IPS: Intrusion Protection System
IntTrl: Interface Translation
JIA: Joint Information Assurance
LDAP: Lightweight Directory Access Protocol
OCSP: Online Certificate Status Protocol
OOB: Out-of-Band network
RCVS: Robust Certificate Validation Service
SaaS: Software-as-a-Service WAF: SRX:
VDC: Virtual Data Center
Web Application Firewall

Figure 7, the ICAP provides connectivity for on-premise CSPs while the BCAP provides connectivity for Off-Premise CSPs. While an off-premise CSP will be allowed to connect directly to a BCAP, a CSP may also connect to a BCAP through a MeetMe Point (MMP). MMPs are commercial facilities where CSP connections may be aggregated for private transport to a BCAP. MMPs may be strategically placed geographically to provide commercial carrier communication aggregation points. The BCAP and MMP are generally referred to together as "CAP/MeetMe". There may be many CAPs and many MMPs that are sized and geographically distributed to optimize network performance. Further, BCAPs and MMPs may not be physically collocated.

The VDSS provides Mission Owner enclave perimeter protections within the Cloud Service Environment (CSE) but also acts as the break and inspect point for traffic capture used by both DISN Boundary and DoD Mission CSSPs and a central peering point for all instantiated virtual network enclaves. Acting as the logical common routing point for cloud enclaves, the VDSS ensures that all traffic entering and leaving every enclave within the CSE will be inspected by the VDSS security stack. This is not to say that all traffic types and routes will receive all levels of inspection. It is assumed that the traffic inspection and logging capabilities of the CSP will be employed to the greatest extent possible.

The VDMS brings the management tools necessary to maintain a compliant security posture for Mission Owner enclaves; also known as Virtual Private Clouds (VPCs). These services may be provisioned from a 3rd party DoD service provider or deployed by the Mission Owner.



Acronyms

ACAS: Assured Compliance Assessment Solutions
CSAAC: Cyber-Situational Awareness Analytic Cloud
ESM: Enterprise Systems Management
FW: Firewall
HBSS: Host-Based Security Services
HSM: Hardware Security Module
IA: Information Assurance
IAP: Internet Access Point
IDS: Intrusion Detection System
IPS: Intrusion Protection System
IntTrl: Interface Translation
JIA: Joint Information Assurance
LDAP: Lightweight Directory Access Protocol
OCSP: Online Certificate Status Protocol
OOB: Out-of-Band network
RCVS: Robust Certificate Validation Service
SaaS: Software-as-a-Service WAF: SRX:
VDC: Virtual Data Center
Web Application Firewall

Figure 7. Notional SCCA System & Connectivity

2.2.1 DISN Connectivity

This section describes the network requirements for establishing DISN network connections to CSEs. Table 7 provides DISN connectivity requirements.

The following assumptions are made with respect to implementation of DISN connectivity.

- CAP connected Mission Owner virtual networks are treated as an extension of the DoD Information Network (DoDIN)
- A CSP may connect to the DISN by one of the following (subject to change):
  a) Direct physical connection to the BCAP or ICAP
  b) MeetMe Point (MMP) for off-premise CSPs.
- Established MMPs will provide direct connectivity into the CSP's private network.

Table 7. DISN Connectivity Requirements

Req. ID	DISN Connectivity Requirements
2.2.1.1	The BCAP and ICAP shall extend the DoDIN into the virtual network of the Cloud Service Environment (CSE)
2.2.1.2	The BCAP shall provide a network connection to established MeetMe Points in order to route DISN traffic to impact level 4 & 5 mission applications hosted in Off-Premise CSEs
2.2.1.3	The MeetMe facility shall provide the capability to host a DISN endpoint router and provide cross connect transport to a CSP router
2.2.1.4	The BCAP shall provide a capability to simultaneously connect to multiple CSPs via a MeetMe Point
2.2.1.5	The BCAP/ICAP and CSP network connections shall be designed to ensure network traffic follows CC/S/A routing policies
2.2.1.6	The BCAP shall connect to the DISN and MeetMe Point using DISN Transport or a secure leased line
2.2.1.7	The BCAP/ICAP and VDSS shall support IPv4 (native, implemented through a dual-stack approach for compatibility with IPv6, as needed)
2.2.1.8	The BCAP/ICAP shall maintain logical network segmentation between Impact Levels 4 & 5 traffic flows passing to and from CSP systems.

2.2.2 Mission Application Connectivity

DoD Mission Owner applications reside within a CSE operating at Impact Levels 4/5 will be accessible only via the CAP/MeetMe-VDSS component combination. Table 8 identifies mission application connectivity requirements.

The following assumptions are made with respect to implementation of mission application connectivity[14]:

- The DISN will be extended to the CSP
- All traffic bound for the Internet will traverse the BCAP/ICAP and IAP
- DISN traffic will traverse a BCAP/ICAP
- DISN traffic leverages NIPRNet transport to the BCAP/ICAP and commercial carriers to the CSP
- Mission applications may be Internet facing; Internet Facing Applications (IFAs) can be non-restricted or restricted (requiring CAC authentication).
- DoD users on the Internet may first connect into their assigned DISN Virtual Private Network (VPN) network before accessing a DoD private applications. IFAs, may be accessed by Internet user through the IAP and traversing the BCAP/ICAP.

Table 8. Mission Application Connectivity

Req. ID	Mission Application Connectivity Requirements (Impact Level 4/5)
2.2.2.1	User traffic to/from the NIPRNet to/from a commercial CSO shall traverse a CAP (BCAP or ICAP)
2.2.2.2	The MeetMe Point shall be a termination and aggregation point for connections to the DISN originating from Off-Premise CSPs unless a CSP is connected directly to the BCAP
2.2.2.3	The BCAP/ICAP shall implement and maintain logical network separation of Internet-sourced traffic for IFA from NIPRNet-sourced traffic

2.2.3 Management Network Connectivity for Off-Premise CSO

As illustrated in Figure 8, three (3) management networks exist within the CSP: 1) CSP's Management Networks (used by CSP operators to manage the CSE), 2) Customer Portal (used by DoD Mission Owner privileged users to typically provision IaaS and PaaS CSO services), and 3) The VDMS (typically used by DoD Mission Owner privileged users to manage systems deployed to the IaaS and PaaS CSE). The CSP's Management Network is private and accessible only via CSP personnel. The Customer Portal is provided to the DoD Mission Owner by the CSP for the purpose of provisioning and configuring CSOs. Service end-points for Application Program Interfaces (API) and Command Line Interfaces (CLI) are generalized as part of the Customer Portal network. These systems can be accessed through the internet by DoD privileged users only (e.g., DoD system and network administrators). The VDMS is employed by DoD

[14] DoD CC SRG

Mission Owner privileged users (e.g., DoD system and network administrators) and is accessible only via the CAP. Table 9 provides management network connectivity requirements for the SCCA.

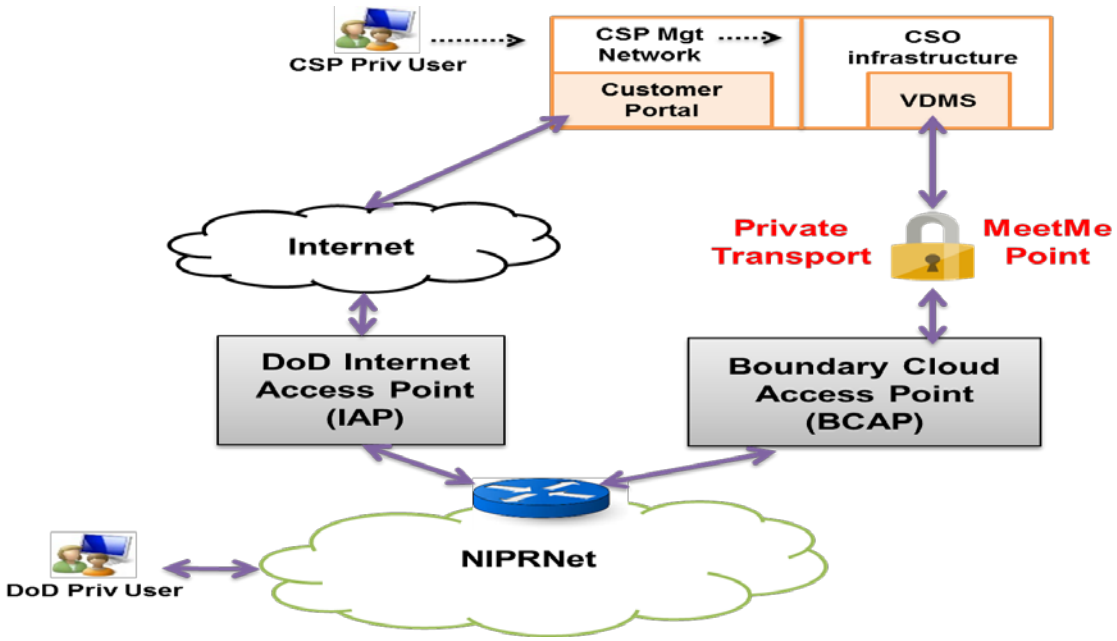


Figure 8. Management Network Connectivity for Off-Premise CSO

The following assumptions are made with respect to implementation of management connectivity:

- Mission Owners are able to use DISN management networks for management of resources within their CSE consistent[15]
- Transfer of CSP originated cybersecurity event and vulnerability data from CSP is performed via the Defense Industrial Base (DIB) network
- IaaS and PaaS CSOs will provide a mechanism to create a mission owner management network within the virtual network of the CSO
- The Customer Portal will be addressed via Public-IP
- The VDMS will be addressed via DoD-IP
- Virtual systems deployed into the CSE will achieve connectivity to user, data, and management networks through the use of logically separate and distinct virtual network interface capabilities.
- Mission Owner Management Network traffic for impact levels 4 and 5 traverses the BCAP; the DISN and CSP management networks are separate and distinct in accordance with the JIE JMN[16]

[15] JMN EDS
[16] JMN EDS

Table 9. Off-Premise Management Network Connectivity

Req. ID	Management Connectivity Requirements
2.2.3.1	The VDMS enclave shall form the DISN management network within the CSE
2.2.3.2	The VDMS shall allow DoD privileged user access to mission owner management interfaces inside the CSO
2.2.3.3	The VDMS shall provide secure connectivity to mission owner management systems inside the CSO that is logically separate from mission application traffic.

2.2.4 Management Network Connectivity for On-Premise CSO

As illustrated in Figure 8, three (3) management networks exist within the CSP: 1) The CSP's Management Networks (used by CSP operators to manage the CSE), 2) The Customer Portal (used by DoD Mission Owner privileged users to typically provision IaaS and PaaS CSOs), and 3) The VDMS (typically used by DoD Mission Owner privileged users to manage systems deployed to the IaaS and PaaS CSE). The CSP's Management Network is private and accessible only via CSP personnel. The Customer Portal is provided to the DoD Mission Owner by the CSP for the purpose of provisioning and configuring CSOs. Service end-points for Application Program Interfaces (API) and Command Line Interfaces (CLI) are generalized as part of the Customer Portal network. These systems may be accessed directly via the ICAP by DoD privileged users only (e.g., DoD system and network administrators). The VDMS may be employed as a means of extending the DoD management network into the on-premise CSP if other equivalent means are not provided by the Mission Owner or CSP. Table 10 provides SCCA management network connectivity requirements for support to the on-premise CSP.

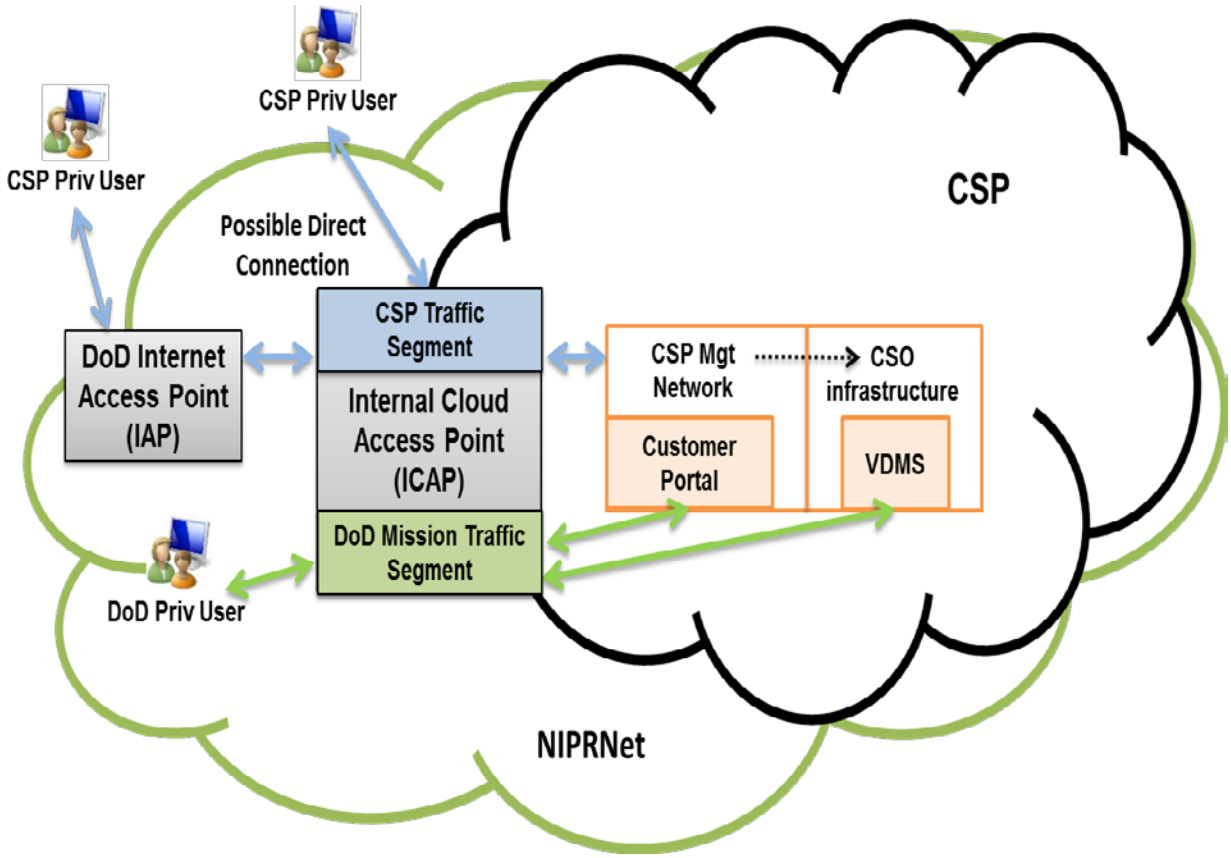


Figure 9. Management Network Connectivity for On-Premise CSO

The following assumptions are made with respect to implementation of management connectivity:

- Mission Owners are able to use DISN management networks for management of resources within their CSE[17]
- Transfer of CSP originated cybersecurity event and vulnerability data from CSP's management network is performed via channels specified by the assigned DoD CSSP
- IaaS and PaaS CSOs will provide a mechanism to create a mission owner management network within the virtual network of the CSO
- A DoD Mission Owner may establish a virtual management network within the CSO delivered by the CSP. As such, the VDMS may not necessarily be deployed into the CSO
- The on-premise CSP will employ DoD-IP addresses for all systems and services associated with delivered CSOs. Accordingly:

[17] JMN EDS

  - The Customer Portal will be addressed via DoD-IP
  - The DoD management environment within the CSO and/or the deployed VDMS will be addressed via DoD-IP
- Mission Owner Management Network traffic for impact levels 4 & 5 traverses the ICAP; the DISN and CSP management networks are separate and distinct in accordance with the JIE JMN.[18]

Table 10. On-Premise Management Network Connectivity

Req. ID	Management Connectivity Requirements
2.2.4.1	The ICAP shall provide secure connectivity to the mission owner established virtual management networks inside the CSO; This network may or may not be implemented by the VDMS
2.2.4.2	The ICAP shall allow secure client access to the by CSP privileged users to CSP owned and operated management network.
2.2.4.3	The ICAP shall allow the transfer of security sensor data from the mission owner virtual networks to the DISN management network
2.2.4.4	The ICAP shall provide network traffic isolation between the CSP's privileged user (i.e., CSP Personnel) management network and DoD Mission Owner virtual networks.
2.2.4.5	(Optional) The VDMS enclave shall form the DISN management network within the CSE and provide the same capabilities identified in Table 9.

2.2.5 Optional Cyber Security and Interface Translation

The CAP will optionally provide a capability to translate network interfaces for specific CSOs. Table 11 provides DISN network interface and translation requirements. Optional requirements can be implemented at either the ICAP or the BCAP.

The following assumptions are made with respect to implementation of a DISN network interfaces and translations:

- Media traffic is restricted to NIPRNet and Public Switched Telephone Network (PSTN) traffic uses the DoD Voice-ISP service not a CSP provided service.
- The cloud service may integrate with the DoD unclassified telephone network (i.e., DSN or Enterprise-Voice over Internet Protocol (VoIP)) via VoIP (Session initiation Protocol (SIP) trunking)

[18] JIE EOC EDS

- A cloud service may host a VoIP solution where the session controller is in the CSP supporting hardware based telephones or softphones on NIPRNet such that DISN endpoints may not be integrated within a collaboration application
- A CSP may be unable to reconfigure assigned host IP interface addresses from public IP to DoDIN IP ranges.

Table 11. Optional Cyber Security and Interface Translation

Req. ID	Interface and Translation Requirements
2.2.5.1	(Optional) The CAP shall provide the capability to detect and/or prevent VoIP call eavesdropping, modification, and hijacking when interfacing DISN to CSP hosted VoIP systems
2.2.5.2	(Optional) The CAP shall provide the capability to support all enterprise level Session Border Controller (SBC) capabilities and functions as defined in the Unified Capabilities Requirements (UCR) 2013[19] when interfacing DISN to CSP hosted VoIP and SIP systems
2.2.5.3	(Optional) The CAP shall provide the capability to terminate VoIP signaling sessions such as the Session Initiation Protocol (SIP) or Assured (AS)-SIP as a back-to-back user agent when interfacing DISN to CSP hosted VoIP systems
2.2.5.4	(Optional) The BCAP and ICAP shall provide the capability to terminate/Decrypt and initiate/encrypt VoIP (e.g., SIP/AS-SIP) signaling sessions secured with Transport Layer Security (TLS) when interfacing DISN to CSP hosted SIP systems
2.2.5.5	(Optional) The BCAP and ICAP shall provide the capability to dynamically manage the opening and closing of User Datagram Protocol (UDP) ports carrying Real-time Transport Protocol (RTP)/RTP Control Protocol (RTCP) media streams
2.2.5.6	(Optional) The BCAP and ICAP shall provide the capability to decrypt and encrypt VoIP media streams using Secure RTP (SRTP)/ Secure RTCP (SRTCP) when interfacing DISN to CSP hosted VoIP systems
2.2.5.7	(Optional) The BCAP and ICAP shall provide the capability to support interoperability with the Enterprise-VoIP service on NIPRNet by signaling with AS-SIP-TLS and encrypting media using SRTP when interfacing DISN to CSP hosted VoIP systems
2.2.5.8	(Optional) The BCAP and ICAP shall provide the capability to support monitoring of VoIP signaling and alerting to CND capabilities when interfacing DISN to CSP hosted VoIP systems
2.2.5.9	(Optional) The BCAP shall provide network address translation (NAT) to translate public IP to DISN IP when Software-as-a-Service (SaaS) CSOs require the use of public IP.

[19] DoD UCR 2015

Req. ID	Interface and Translation Requirements
2.2.5.10	(Optional) The BCAP shall provide secure DNS proxy to support cloud hosted system URL resolution of public IP space using DISN IP translation
2.2.5.11	(Optional) The BCAP shall provide break and inspection capability of application layer traffic (to include SSL/TLS) for boundary CND purposes (e.g. forward proxy)
2.2.5.12	(Optional) The BCAP and ICAP shall provide direct connectivity of CSP provided email exchange services to the DoD EEMSG for the purposes of email hygiene inspection

2.3 Mission Support System Requirements

2.3.1 Mission Applications

SCCA components will be built to accept, pass, and interoperate with mission owner applications that are compliant with DoD system and data center STIGs. Table 12 provides mission application integration requirements.

The following assumptions are made with respect to implementation of a DoD mission application integration:

- SCCA documentation will provide information detailing common and hybrid security controls which are eligible for adoption and inheritance by mission systems
- The BCAP and ICAP will be accredited as a networking component of the DISN
- VDSS and VDMS Assessment and Authorization will be performed separately by the VDSS and VDMS providers in accordance with the DoD Cloud Computing SRG.

Table 12. Integration with Mission Applications

Req. ID	Integration with Mission Applications Requirements
2.3.1.1	The BCAP, ICAP, and VDSS shall allow approved ports and protocols communications to include whitelisted mission application traffic & services access from Internet via the DISN Internet Access Point (IAP)
2.3.1.2	The VDSS shall provide CSO resident or remotely hosted mission enclave perimeter protection and sensing
2.3.1.3	The BCAP, ICAP, and VDSS shall allow secure connections to the mission owner application enclave for user plane traffic sourced from within the DISN or the Internet via the IAP
2.3.1.4	The BCAP, ICAP, and VDSS shall provide for logical separation of mission owner application networks

2.3.2 Component Management

SCCA components will be built to integrate with existing DoD Computer Network Defense (CND) and administration systems, capabilities, and networks. Component Management is concerned with managing the health, status, and configuration of SCCA systems. Table 13 provides SCCA component management requirements.

The following assumptions are made with respect to implementation of SCCA component management capabilities:

- SCCA management systems will be hosted within and accessible via the DISN management network and the DISA datacenter management networks.
- SCCA management systems will ensure consistency between SCCA primary and failover systems

Table 13. Component Management Requirements

Req. ID	Component Management System Requirements
2.3.2.1	SCCA components shall provide element managers to manage the configuration of system elements comprising the CAP, VDSS, and the VDMS
2.3.2.2	SCCA component managers shall be able to manage (e.g., set security, configuration, & routing policies and install patches) SCCA system security and network components
2.3.2.3	SCCA component managers shall allow for the configuration, control, and management of Ports, Protocols, and Services Management (PPSM) in accordance with DoDI 8551.01[20]
2.3.2.4	SCCA component managers shall provide a capability to implement and control system configuration, report configuration change incidents, and support DoD Component change configuration management systems and processes
2.3.2.5	SCCA management systems shall support the sharing of Combatant Commands, Services, Agencies (CC/S/A) SIEM event & correlation data with the CC/S/A and CND Service Providers
2.3.2.6	SCCA components shall provide logically separate network interfaces for access from the management network infrastructure that is logically separate from production
2.3.2.7	SCCA components shall support management administration from the DISN management system and/or DISA Datacenter Management System
2.3.2.8	SCCA components shall provide sensor events, performance, and resource utilization metrics to the component operators

[20] DoDI 8551.01 PPSM

Req. ID	Component Management System Requirements
2.3.2.9	SCCA components shall provide for management traffic segmentation from user and data plane traffic

2.3.3 Performance Management

Performance Management is the monitoring and management of performance and availability of SCCA systems and components. Performance Management operates to detect and diagnose complex system performance problems to maintain an expected level of service. SCCA management systems will operate within the management network (DISN or Cloud side) to provide a performance management capability for monitoring the performance and health of SCCA security components. Table 14 provides SCCA performance management requirements.

Table 14. Performance Management Requirements

Req. ID	Performance Management Requirements
2.3.3.1	SCCA security elements (i.e., BCAP, ICAP, VDSS, and VDMS) shall provide a performance management capability to monitor the health and status of security elements.
2.3.3.2	SCCA security elements shall provide performance data, such as CPU, bandwidth, memory and disk I/O, and storage utilization to SCCA management systems for performance analysis and reporting
2.3.3.3	The SCCA security elements shall be able to generate reports and alerts based on performance information provided by SCCA systems.

2.3.4 Security Information & Event Management (SIEM)

Security information and event management (SIEM) technology provides real-time analysis of security alerts generated by SCCA hardware and applications. The SIEM capability is implemented by both Boundary and Mission CND service providers to interpret system, user, and application events. The SCCA does not provide a full SIEM capability. However, log aggregation, forwarding, and indexing components must be implemented to integrate with and interoperate with JMN SIEM systems. Table 15 provides SIEM capability requirements.

The following assumptions are made with respect to implementation of a SCCA SIEM support capabilities:

- SCCA management systems will support integration with a SIEM capability that will collect, store, normalize, aggregate and correlate security relevant events from SCCA components
- The SCCA management system will provide an Event Management Capability that collects, stores, and correlates security relevant events

- SCCA generated security information and event data will feed Acropolis and JMN SIEM systems, as required to support CSSP operations.

Table 15. Security Information & Event Management Requirements

Req. ID	SIEM Requirements
2.3.4.1	SCCA elements shall support the delivery of security relevant events through element management ports
2.3.4.2	SCCA elements shall support CC/S/A unique tagging of events
2.3.4.3	SCCA elements shall provide a checksum mechanism to detect the unauthorized alteration of event information during transmission of event data
2.3.4.4	SCCA elements shall securely provide security relevant events to SCCA element management systems for logging, filtering, and correlating
2.3.4.5	SCCA elements shall support caching of security relevant events if logging of events is not available
2.3.4.6	SCCA shall provide BCP and MCP operator access to security information and security relevant event data derived from SSL/TLS session traffic which is broken and inspected at the VDSS and ICAP
2.3.4.7	SCCA shall feed specifically identified security information and security relevant event data necessary for situational awareness (SA) to Acropolis

2.3.5 Full Packet Capture (FPC)

Full Packet Capture (FPC) is used during analysis of event traffic by the SIEM capability. The capability will capture, store, and provide event correlated session traffic back to the SIEM for use by CND Service Providers engaged in both Boundary and Mission defense. The FPC capability will be implemented at the break and inspection points to provide the greatest CND visibility and situational awareness. However, since FPC may be performed at multiple points within the DISN to include JRSS, the IAP, and the Core Data Centers, the FPC function of the VDSS is intended to be configurable according to traffic flow source and destination points to avoid multiple point capture. Additionally, depending upon the capabilities available within the CSO, FPC equivalent data may also be captured within the CSE. Table 16 provides FPC capability requirements.

The following assumptions are made with respect to implementation of SCCA FPC capabilities:

- FPC data captured in the CSE will be stored within the CSE.
- FPC data will not be archived except to support forensic investigations.

Table 16. Full Packet Capture (FPC) Requirements

Req. ID	Full Packet Capture (FPC) Requirements
2.3.5.1	The FPC shall support integration with SIEM systems to effect data search and retrieval, such as the capability to pull select timeframes of captured data
2.3.5.2	The FPC shall provide the means to reconstruct all network traffic sessions traversing the SCCA Component.
2.3.5.3	The FPC shall provide defined data queries that run against metadata
2.3.5.4	The FPC shall provide a capability to request an arbitrary subset of packets
2.3.5.5	The FPC shall locally store captured traffic for 30 days
2.3.5.6	The FPC data shall be isolated from user and data plane traffic via cryptographic or physical means
2.3.5.7	The FPC data shall be query-able from a secure remote location on the management network
2.3.5.8	The FPC function shall be configurable according to traffic flow source and destination points to avoid multiple point capture

2.4 Performance Requirements

This section provides the SCCA system quality of service (QoS) and performance requirements. QoS and performance requirements affecting the CSP infrastructure and service offerings will be defined by Service Level Agreement (SLA) between the CSP and the acquiring DoD Mission Owner at the time of procurement. Specifications on CSO performance are out of scope for this document.

The following assumptions are made with respect to implementation of SCCA performance requirements:

- The BCAP/ICAP will maintain DISN Service Level Agreement (SLA) objectives[21]
- The BCAP/ICAP and design will not degrade RTT latency performance between DISN nodes as defined in the DISN SLA for Intra-CONUS, Intra-EUR, and Intra-PAC

[21] DISA Network Services Telecommunications SLA

2.4.1 BCAP/ICAP Performance

Table 17 below provides the requirements for CAP performance.

Table 17. BCAP/ICAP Performance Requirements

Req. ID	BCAP/ICAP Performance Requirements
2.4.1.1	The BCAP shall support scalability of up to 10 Gigabit/second throughput between the DISN and CSP
2.4.1.2	The ICAP shall start with 1 Gigabit/second throughput and have ability to scale up to 10G.
2.4.1.3	The BCAP/ICAP shall support assured bandwidth (Quality of Service)
2.4.1.4	The BCAP/ICAP shall support IP packet forwarding in accordance with Mission Owner Differentiated Services Code Point (DSCP) tagged QOS prioritization
2.4.1.5	The BCAP/ICAP shall meet NIPRNet backbone availability of 99.5%
2.4.1.6	The BCAP/ICAP unit processing latency shall be no greater than 35 milliseconds
2.4.1.7	The BCAP (location/performance) design shall provide Round-Trip Time (RTT) in accordance with DISN SLA latency between the CSP and DISN services nodes: <100msec for Intra-CONUS <150msec for Intra-EUR <150msec for Intra-PAC (Oahu, HI-Western Pacific)
2.4.1.8	The BCAP/ICAP unit packet loss shall be <1%

2.4.2 VDSS Performance

Table 18 provides the requirements for VDSS Performance.

Table 18. VDSS Performance Requirements

Req. ID	VDSS Performance Requirements
2.4.2.1	The VDSS unit processing latency shall be no greater than 35 milliseconds
2.4.2.2	The VDSS unit packet loss shall be <1%

Req. ID	VDSS Performance Requirements
2.4.2.3	The VDSS shall achieve availability of 99.5%
2.4.2.4	The VDSS shall support NIPRNet assured bandwidth (Quality of Service) for mission owner systems residing within the commercial cloud
2.4.2.5	The VDSS shall support IP packet fowarding in accordance with Mission Owner Differentiated Services Code Point (DSCP) tagged QOS prioritization

2.4.3 VDMS Performance

Table 19 provides the requirements for VDMS performance.

Table 19. VDMS Performance Requirements

Req. ID	VDMS Performance Requirements
2.4.3.1	The VDMS shall achieve availability of 99.5%

2.5 Continuity of Operations Requirements

SCCA components will support DoD Continuity of Operations Plans (COOP) to ensure that DoD components are able to continue performance of essential functions under a broad range of system outage circumstances.

The following assumptions are made with respect to implementation of continuity of operations solutions:

- DISN routing will support dynamic allocation of traffic between multiple CAP/MeetMe points
- Virtualized SCCA elements will be designed to achieve the COOP needs of supported Mission Owner segments.

2.5.1 BCAP/ICAP Continuity of Operations

Table 20 provides the requirements for the CAP Continuity of Operations.

Table 20. BCAP/ICAP Continuity of Operations Requirements

Req. ID	BCAP/ICAP Continuity of Operations Requirements
2.5.1.1	In the event of a catastrophic site failure, the ICAP and BCAP/MeetMe shall allow the failover of functionality from one site to another with minimum impact to mission user application traffic and mission owner management traffic. The amount of time needed to failover a site should be less than 30 seconds once initiated.

Req. ID	BCAP/ICAP Continuity of Operations Requirements
2.5.1.2	The BCAP/ICAP shall maintain online backup configurations for recovery of operations
2.5.1.3	The BCAP/ICAP management systems shall provide a mechanism for managing failover
2.5.1.4	The BCAP/ICAP management systems shall provide the capability to ensure all SCCA element configurations and policies are recoverable
2.5.1.5	The BCAP/ICAP shall maintain offsite backup configurations for the recovery of operations

2.5.2 VDSS Continuity of Operations

Table 21 provides the requirements for VDSS Continuity of Operations.

Table 21. VDSS Continuity of Operations Requirements

Req. ID	VDSS Continuity of Operations Requirements
2.5.2.1	The VDSS management systems shall provide a mechanism for managing failover in accordance with DoD UCR 2013.
2.5.2.2	The VDSS management systems shall provide the capability to ensure all SCCA element configurations and policies are recoverable
2.5.2.3	The VDSS shall maintain offsite backup configurations for the recovery of operations

2.5.3 VDMS Continuity of Operations

Table 22 provides the requirements for VDMS Continuity of Operations.

Table 22. VDMS Continuity of Operations Requirements

Req. ID	VDMS Continuity of Operations Requirements
2.5.3.1	The VDMS management systems shall provide a mechanism for managing failover
2.5.3.2	The VDMS management systems shall provide the capability to ensure all SCCA element configurations and policies are recoverable

Req. ID	VDMS Continuity of Operations Requirements
2.5.3.3	The VDMS shall maintain offsite backup configurations for the recovery of operations

2.6 System Scalability Requirements

SCCA components will be built to support scalability both horizontally (add processing components) and vertically (add resources to processing components) to handle a growing amount of work or to improve system performance. Scalability solutions may also address the number and location of nodes.

The following assumptions are made with respect to implementation of SCCA scalability requirements:

- The active and passive security elements, bandwidth, application session demand, and number of SCCA security components will change over time

CAP/MeetMe node location and distribution will be a factor considered for maintaining the DISN Service Level Agreement SLA[22]; not all CSPs will be reachable from a single CAP/MeetMe point.

2.6.1 BCAP/ICAP Scalability

Table 23 provides the requirements for CAP Scalability.

Table 23. BCAP/ICAP Scalability Requirements

Req. ID	CAP Scalability Requirements
2.6.1.1	The BCAP/MeetMe shall be designed to scale to meet the bandwidth and session demands of all projected CSO hosted mission applications and to support accessibility by multiple CSPs
2.6.1.2	In the event of a failover, the surviving BCAP/MeetMe at an alternate site shall have sufficient capacity to meet the combined bandwidth and session demands of its own plus those failed over from the other site
2.6.1.3	The BCAP/ICAP shall support scalability of up to 10 Gigabit/second throughput at all points within the design

2.6.2 VDSS Scalability

Table 24 provides the requirements for VDSS scalability.

[22] DISA Network Services Telecommunications SLA

Table 24. VDSS Scalability Requirements

Req. ID	VDSS Scalability Requirements
2.6.2.1	The VDSS shall be designed to rapidly scale virtual elements up and down in capacity to achieve negotiated (between components provider and Mission Owner) SLA objectives while minimizing metered billing CSO costs incurred by DoD procuring component
2.6.2.2	The VDSS shall support scalability in increments of 1 Gigabit/second throughput at all points within the design without costly modification

2.6.3 VDMS Scalability

Table 25 provides the requirements for VDMS Scalability.

Table 25. VDMS Scalability Requirements

Req. ID	VDMS Scalability Requirements
2.6.3.1	The VDMS shall be designed to rapidly scale virtual elements up and down in capacity to achieve negotiated (between components provider and Mission Owner) SLA objectives while minimizing metered billing CSO costs incurred by DoD procuring component

2.7 Backup and Restoration Requirements

The SCCA components will be built to provide a mechanism to perform regularly scheduled backup of SCCA system binaries and configurations as well as the ability to fully restore SCCA system components to their last known good configuration. Backup and restoration requirements apply to SCCA systems only.

The following assumptions are made with respect to implementation of SCCA backup and restoration requirements:

- Backup systems are protected in accordance with DoD end-point protection policies.

BCAP/ICAP Backup and Restoration

Table 26 provides the requirements for CAP Backup and Restoration.

Table 26. BCAP/ICAP Backup and Restoration Requirements

Req. ID	BCAP/ICAP Backup and Restoration Requirements
2.7.1.1	The BCAP/ICAP shall provide the ability to backup and restore security, network, account, and system configurations

Req. ID	BCAP/ICAP Backup and Restoration Requirements
2.7.1.2	The BCAP/ICAP shall provide the capability to backup configuration and system data of all SCCA elements
2.7.1.3	The BCAP/ICAP shall provide the means to restore operational capability

2.7.1 VDSS Backup and Restoration

Table 27 provides the requirements for VDSS Backup and Restoration.

Table 27. VDSS Backup and Restoration Requirements

Req. ID	VDSS Backup and Restoration Requirements
2.7.2.1	The VDSS shall provide the ability to backup and restore security, network, account, and system configurations
2.7.2.2	The VDSS shall provide the capability to backup configuration and system data of all VDSS elements
2.7.2.3	The VDSS shall provide the means to restore operational capability

2.7.2 VDMS Backup and Restoration

Table 28 provides the requirements for VDMS Backup and Restoration

Table 28. VDMS Backup and Restoration Requirements

Req. ID	VDMS Backup and Restoration Requirements
2.7.3.1	The VDMS shall provide the ability to backup and restore security, network, account, and system configurations
2.7.3.2	The VDMS shall provide the capability to backup configuration and system data of all VDMS elements
2.7.3.3	The VDMS shall provide the means to restore operational capability

Appendix A: Acronyms and Abbreviations

Acronym/Abbreviation	Explanation
AV	Attack Vector
BCAP	Boundary Cloud Access Point
BCDP	Boundary Cyber Defense Provider
CCMP	Cloud Credential Management Plan
C-CSP	Commercial Cloud Service Provider
CAP	Cloud Access Point
CC/S/A	Combatant Command/Service/Agency
CDC	Core Data Center
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COOP	Continuity of Operations
CSE	Cloud Service Environment
CSO	Cloud Service Offering
CSP	Cloud Service Provider
CSS	CSP Security Stack
CUI	Controlled Unclassified Information
DISA	Defense Information Systems Agency
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDIN	DoD Information Network
DISN	Department of Defense Information Network
DDOS	Distributed Denial of Service

Acronym/Abbreviation	Explanation
DOS	Denial of Service
EEMSG	Enterprise Email Security Gateway
FIPS	Federal Information Processing Standards
FPC	Full Packet Capture
FRD	Functional Requirements Document
HBSS	Host Based Security Services Program
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
IaaS	Infrastructure as a Service
IAP	Internet Access Point
ICAP	Internal Cloud Access Point
JMS	Joint Management System
MCDP	Mission Cyber Defense Provider
MMP	MeetMe Point
NFG	NIPRNet Federated Gateway
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSS	National Security System
PaaS	Platform as a Service
PKI	Public Key Infrastructure
RMF	Risk Management Framework
SaaS	Software as a Service
SARM	Security Architecture Reference Model
SCCA	Secure Cloud Computing Architecture
SIEM	Security Information and Event Manager
SIP	Session Initiation Protocol

Acronym/Abbreviation	Explanation
SOPP	Service Ordering and Provisioning Portal
SRG	Security Requirements Guide
SRTP	Secure Real-Time Protocol
STIG	Security Technical Implementation Guides
TLS	Transport Layer Security
TCCM	Trusted Cloud Credential Manager
URL	Uniform Resource Locator
USCYBERCOM	United States Cyber Command
VDMS	Virtual Datacenter Managed Service
VDSS	Virtual Datacenter Security Stack
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMM	Virtual Machine Manager
VoIP	Voice over IP
VPN	Virtual Private Network

Appendix B: Threat Definitions

Advanced Persistent Threat - A set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific IT asset.

Cross-VM Attack – A threat vector whereby the threat actor seeks to acquire information from or disrupt operations of a collocated adjacent tenant Virtual Machine (VM).

CSP Resource Non-Compliant Configuration (Non-Compliance Activity) - A detectable presence or persistence of an application, operating system, or platform vulnerability that is exploitable by an attacker

Data Exfiltration - Unauthorized copying, transfer or retrieval of data from a computer or server.

Denial of Service - A threat vector whereby a network of automated attack platforms operate synchronously to consume available system resources, bind the operations of a system, and/or otherwise disrupt normal system operations. This is also known as a distributed denial-of-service (DDoS) where the attack source is more than one–and could be thousands–of unique IP addresses. A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. This definition also addresses CSP owned and operated resources.

DNS Hijacking (CSO hosted app DNS request) - A threat vector whereby is an attacker acts to subvert the resolution of Domain Name System (DNS) queries. This can be achieved by malware that overrides a computer's TCP/IP configuration to point at a rogue DNS server under the control of an attacker, or through modifying the behavior of a trusted DNS server so that it does not comply with internet standards.

IP Address Spoofing - A threat vector whereby an attacker seeks to achieve network access through the creation of Internet Protocol (IP) packets with a forged source IP address, for the purpose of concealing the identity of the sender or impersonating another computing system.

IP Route Hijacking - A threat vector where an attacker seeks the illegitimate takeover of groups of IP addresses by corrupting routing tables; aka: IP Hijacking, BGP hijacking, prefix hijacking or route hijacking.

Malicious Code/Malware (Malicious Logic) - A threat vector for which an attacker seeks the exploitation of a computer bug that is caused by processing invalid data. Malicious code, malware, or logic Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution.

Network Enumeration - The unauthorized scanning of network assets for the purpose of discovering system vulnerabilities through to mount an attack

Pooled Resource Data Leakage (User Intrusion) - A threat vector whereby the shared storage, memory, and/or compute resource of the virtualization environment are exploited by a neighbor tenant to yield unauthorized information disclosure.

Rogue Access Device/AP Hijack (com carrier traffic interception or adding to IaaS LAN) - A threat vector whereby an illegitimate network device is installed on a secure network without explicit authorization from the network administrator, whether added by a well-meaning employee or by a malicious attacker.

Session Hijack/Man-In-The Middle – A threat vector whereby an attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Service Account Hijack – A threat vector whereby CSP service account credentials are compromised and an attacker gains unauthorized access and root privileges of the cloud service account established to support provisioning of cloud systems by the cloud consumer.

SQL Injection - A code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

Unauthorized CAP Privileged User Account Access Perimeter - A threat vector whereby for which the result is to provide unauthorized access to privileged user accounts.

Unauthorized TCP/IP Source/Destination - A threat vector whereby and attacker seeks to execute an exploit or gain access to a network through an unauthorized TCP port or IP address.

Unauthorized Virtual Machine Management Console Access (Root Intrusion) - A threat vector whereby privileged user access the Virtual Machine Management (VMM) interface is achieved.

Virtual Machine Hijack (Root Intrusion) - A threat vector whereby the threat actor seeks to acquire privileged access to and control over a virtual machine.

Virtual Machine (VM) Escape – A threat vector whereby the threat actor seeks to break-out of a servicing Virtual Machine (VM) which is collocated with other tenant's, to subvert operations of the underlying shared virtualization environment, physical host, or other cloud resources.

Virtual Local Area Network (VLAN) Hopping - A method of attacking networked resources on a Virtual LAN (VLAN). The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging.

VoIP Call Eavesdropping - A threat vector whereby an attacker seeks to capture, interpret, and/or record a Voice over Internet Protocol (VoIP) call session.

VoIP Call Hijacking - A threat vector whereby an attacker seeks to intercept and take control of a user Voice over Internet Protocol (VoIP) call session on a particular host, communicating with another host.

VoIP Call Modification - A threat vector whereby an attacker seeks to capture and modify the contents of a Voice over Internet Protocol (VoIP) call session.

VoIP System DOS - A threat vector whereby an attacker seeks to disrupt functionality or limit availability of the Voice over Internet Protocol (VoIP) system.

Appendix C: Cloud Component Terminology[23]

CAP refers to a component of the SCCA designed to provide DISN boundary defense

Commercial CSP (C-CSP) refers to a Non-DoD Non-Federal Government organization offering cloud services to the public and/or government customers as a business, typically for a fee with the intent to make a profit.

CSO refers to a CSP's Cloud Service Offering (recognizing that a CSP may have multiple offerings).

CSE refers to the cloud-computing environment within a CSP

CSP by itself refers to any or all Cloud Service Providers, DoD or non-DoD.

CSS, CSP Security Stack, by itself refers to the perimeter protections provided by the cloud service provider.

DoD CSP refers to a DoD owned and operated CSP, such as the DISA milCloud offering.

DoDIN The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The DoDIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems (NSS). Non-DoDIN Information Technology (IT) includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

DISN The globally interconnected DoD enterprise telecommunications transport network infrastructure. It is integrated and configured to provide long-haul information transfer services for all Department of Defense activities. It provides/supports dedicated point-to-point, switched voice and data, imagery, and video teleconferencing services.

Federal Community Cloud: Is a multi-tenant cloud in which services are provided for the exclusive use of the DoD and Federal Government organizations. Resources providing the cloud services must be dedicated to Federal Government use and require physical separation from non-DoD/non-Federal customers.

Impact Levels are cloud information security levels defined by the combination of: 1) the type of information 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 DoD data, systems or networks. DoD Mission Owners categorize mission information systems in accordance with DoDI 8510.01 and CNSSI 1253 to select the impact level that most closely aligns with defined baselines.

MeetMe Point refers to a place within a colocation center where CSP's and DoD can physically connect to one another and exchange data.

[23] DoD Cloud Computing Security Requirements Guide (CC SRG)

Mission Owners are entities such as program managers within the DoD Components responsible for instantiating information systems and applications leveraging a CSP's Cloud Service Offering.

Non-DoD CSP refers to a commercial or Federal Government owned and operated CSP.

Off-premises commercial data centers, systems, and CSPs operating within facilities that are not under the direct control of the DoD.

On-premises includes DoD data centers, authorized commercial data centers, other facilities located on a DoD Base, Camp, Post and Station (B/C/P/S), or in a commercial or another government facility (or portions thereof) under the direct control of DoD personnel and DoD security policies.

Private Cloud: Is a cloud in which services are provided for the exclusive use of the DoD; supporting multiple DoD tenants or DoD sponsored tenants in the same cloud. The DoD maintains ultimate authority over the usage of the cloud services, and any non-DoD use of services must be authorized and sponsored through the DoD. Resources providing the cloud services must be dedicated to DoD use and have physical separation from resources not dedicated to DoD use. Common Services are capabilities provided as a service to a broad range of mission application owners, such as infrastructure (e.g., domain name service and directories) or security (e.g., enclave security scanning and endpoint protection) services.

VDMS refers to the Virtual Data-Center Management Services component of the SCCA designed to provide end-point protections for mission owner applications such as DoD ACAS, HBSS, IDAM, etc.

VDSS refers to the Virtual Data-Center Security Stack component of the SCCA designed to provide mission owner system defense.