Update on Cloud Cyber Defense CONOPS

Rob Mawhinney
Chief, CyDef Effectiveness Branch
22 April 2016
The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government. This brief may also contain references to Unite States Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments.
The intent of this brief is to provide an overview of all levels as described in the Cloud Cyber Defense CONOPS, to include the C2 and C3 constructs for Cyber Defense.

Defines reporting and data-sharing relationships between the Cyber Defense and Cloud organizations.

It assigns procedures to be performed in response to incidents and events as categorized by DoD.

Introduces the supporting organizations and reference procedures for Cyber Defense of the DoDIN with regards to the cloud:

Expands on the SRG with the introduction of:
• Cloud Cyber Defense C2 Model
• Cloud Cyber Defense C3 Information Sharing Model

The Cloud Cyber Defense Concept of Operations is meant to “evolve as the procedures are put into practice and new best practices emerge.”
## Proposed Lexicon

<table>
<thead>
<tr>
<th>Old Term (6510)</th>
<th>New Term (8530)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CND= Computer Network Defense</td>
<td>CyDef = Cyber Defense</td>
</tr>
<tr>
<td>CNDS = Computer Network Defense Services</td>
<td>CyDef Services = Cyber Defense Services</td>
</tr>
<tr>
<td>CNDSP = Computer Network Defense Service Provider</td>
<td>CDSP = Cyber Defense Service Provider</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Old CONOPS Role Name</th>
<th>Proposed CONOPS Role Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCND = Boundary Computer Network Defense</td>
<td>BCD = Boundary Cyber Defense</td>
</tr>
<tr>
<td>DoDIN CND= DoDIN Computer Network Defense</td>
<td>DCD = DoDIN Cyber Defense</td>
</tr>
<tr>
<td>MCND = Mission Computer Network Defense</td>
<td>MCD = Mission Cyber Defense</td>
</tr>
</tbody>
</table>

Per Joint Pub 3-12, the move is to replace Computer Network Defense (CND) with "Cyber Defense" terminology.
DoDIN Cyber Defense (DCD Functions)

• The primary objective is to monitor for DoDIN-wide attacks
• Builds a broad Cyber SA picture across Missions, MCDs, BCDs, CSOs, and CSPs
• Through their broad view, identify broader patterns of incidents or events

Boundary Cyber Defense (BCD)

• The primary objective is to protect the Defense Information Systems Network (DISN) from attacks
• They perform this protection for any of the below connections through approved Cloud Service Providers (CSPs) that can impact the DISN:
  • Public
  • Private
  • Hybrid
  • Community clouds
Cloud Cyber Defense Organizational Construct– cont.

**Mission Cyber Defense (MCD)**
- The primary objective is to defend systems, applications, and/or data hosted in the Cloud
- Defends all connections to the Cloud Service Offering (CSO), whether via:
  - Internal Cloud Access Point (ICAP);
  - Virtual Private Network (VPN);
  - Direct internet access to public servers; or
  - Other

**Mission Owner (MO)**
- Operates, and maintains the mission systems, applications, and/or data (depending on CSO service model, e.g. IaaS, PaaS, or SaaS)
- Is a DoD entity that acquires cloud services and dedicated connections in support of its mission

**Cloud Service Provider (CSP)**
- Operates one or more CSOs in one or more deployment models (IaaS/PaaS/SaaS)
- Reports to the MCD and Mission Owner on incidents/events
Cloud Cyber Defense CONOPS C2/C3 Models

C2 Model

C3 Model

C2 LEGEND
- Directive Authority
- Direct Support
- Direct Report

C3 LEGEND
- Incident Reporting
- CND Information Sharing
Deployment of Cloud Service Offerings

Cloud Cyber Defense CONOPS was written to support deployment on three different Cloud Service Offerings (IaaS, PaaS, SaaS) either Off-Prem or On-Prem.
Cloud Cyber Defense CONOPS was also written to support three different Impact Levels (2, 4, and 5) for each Cloud Service Offering either Off-Prem or On-Prem.

- **Off-Prem CSO Level 2**
  - (Cyber Defense by MCD)

- **Off-Prem CSO Level 4/5**
  - (Cyber Defense by MCD + BCD)

- **On-Prem CSO Level 2/4/5**
  - (Cyber Defense by MCD)

*includes milCloud*
That’s Great - How does it work?

LEGEND

- Directive Authority
- Incident Reporting
- CyDef Information Sharing

- JFHQ-DoDIN
- US-CERT
- CDSP
- Mission Owner / CSP

Compromise discovered
Cloud CyDef CONOPS Approval Process

DoD AO Level Review

DoD Review of Comments
Comments Adjudication

CONOPS v1

DISA Internal TTX
Comments Adjudication

CONOPS v2

Industry Review

Prep for Cloud Cyber Defense TTX
DoD/Industry Cloud TTX
Incorporation of Final Comments
CSERG Review

CONOPS v3

Industry / DoD Review

DoD-CIO Review

DoD CIO Final Review
DoD-CIO CONOPS Approval/Signature

Signed CONOPS

2w 2w 4w 3w 10w 1w 5w

24-July 22-Aug 5-Oct 15-17 Dec 24-Feb 2-Mar 08-Apr
Next steps to Further Define the Intent, C2, and C3 for CyDef

The Cloud CyDef CONOPS approval process will be replicated for the development of the next three CyDef CONOPS documents.
UNITED IN SERVICE TO OUR NATION
BACK UP Slides
Cloud Cyber Defense CONOPS
Authoritative and Supporting Documents

• DoD Cloud Computing Security Requirements Guide (CC SRG)


• DoD 6510.01B, “Cyber Incident Handling Program”

• Cloud Access Point Functional Requirements Document (CAP FRD)

• DISA Cloud Connection Process Guide (CCPG)
The primary objective is to monitor for DoDIN-wide attacks

**JFHQ-DoDIN, as the DoDIN CyDef (DCD), is accountable to:**

- **Help consolidate related incident tickets**
  - Shall monitor Cyber Defense incident databases (JIMS and DIBNet) for reported incidents
  - Where an incident spans multiple MCDs or BCDs, associate JIMS tickets
  - Determine lead for the activity (e.g. MCD, BCD, or CCMD, etc.)

- **Coordinate with MCDs and BCDs on JFHQ-DODIN orders/tasks status**

- **Pass Intelligence Data**
  - Pass Indications & Warnings (I&W) to BCDs and MCDs
  - Disseminate Threat Intelligence Product Reports (TIPRs) from Intel sources

- **Perform delta of Vulnerability Assessments of CSO-hosted systems, networks, and data**

- **Analyze potential impacts across the multiple Cloud Service Providers**

- **Recommend mitigations**

- **Assigning DoDIN Cyber Protection Teams (CPTs) to focus efforts on a specific threat or adversary.**
The primary objective is to protect the Defense Information Systems Network (DISN) from attacks.

**Boundary Cyber Defense (BCD) is accountable to:**

- **Maintain a CDSP accreditation**
- **Support the MCDs in their objectives of defending their systems, applications, and data hosted in the Cloud**
  - Monitor data in transit through the BCAP based on BCAP sensing capabilities
  - Monitor for unauthorized connections (attempted and actual)
- **Coordinate with MCDs on JFHQ-DODIN orders/tasks status**
  - Pass I&W to MCD, other BCDs, and DCD
  - Disseminate TIPRs from Intel sources
  - Provide aggregated data to DCD
  - Provide BCAP trending data to DCD
  - CCMD/JCC SA coordination
- **Maintain Cyber Situational Awareness (SA) picture across Missions, Cloud Service Offerings (CSOs), and CSPs and can identify broader patterns of incidents or events**
The primary objective is to defend systems, applications, and/or data hosted in the Cloud

**Mission Cyber Defense (MCD) is accountable to:**

- Maintain a CDSP accreditation
- Supports BCD efforts to identify correlations between related incidents or events impacting multiple Missions, CSOs, or CSPs Perform CDSP for the Mission Owner
- Assist Mission Owners with enabling Cyber Defense
- Perform analysis for CSO incidents/events
- Detect CSO events, analyze CSP incidents
- Distribute SAR to DCD and BCDs for Attack Sensing & Warning (AS&W)/SAR
- Distribute guidance/orders (patch management) to Mission Owners
- Retain copy of SLA from Mission Owners; ensure they have proper DoD-approved cloud SLA
Mission Owner

Operates, and maintains the mission systems, applications, and/or data

Mission Owners are accountable to:

• Aligns to an Accredited Provider via MOA/SLA for CyDef services

• Prepare Mission Data for Cyber Defense
  • Ensure Cybersecurity standards are met and in SLA (HBSS, Scans, O&M, STIGs, etc.)
  • Comply with placement of sensors from MCD
  • Ensure feeds of Host Cyber Defense Tools to MCD
  • Add MCD (and BCD for Off-Premise CSOs) to Trusted Disclosure list in SLA

• Reports to MCD on incidents/issues

• Conducts initial Incident Response & Analysis

• Provides lower level Intrusion Detection (IDS) and Monitoring to MCD

• Implements and executes MCD guidance
Cloud Service Providers are accountable to:

- Provides CDSP services for their infrastructure and service offerings
- Support and comply with efforts to resolve issues under the direction of their Mission Owners
- Provide open CSO vulnerability POA&M to Mission Owner
- Maintain current lists of POCs at US-CERT, Mission Owners, and relevant MCDs/BCDs
- Email Mission Owner, BCD, and MCD for alert notification as part of the incident reporting workflow (include DIB ID number, if applicable)
- Meet Continuous Monitoring and Incident Reporting Requirements
- Reports to MCD on incidents/issues
- Conducts initial Incident Response & Analysis, where applicable