DISA
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

The Challenge of Cyberspace Defense and CSSP Services

COL Dee Straub
Chief, DISA Defensive Cyber Operations

Mr. Paul Barbera

Chief, DCO Plans & Requirements

Mr. Rob Mawhinney

Chief, DCO Current Operations

Mr. Darrell Fountain

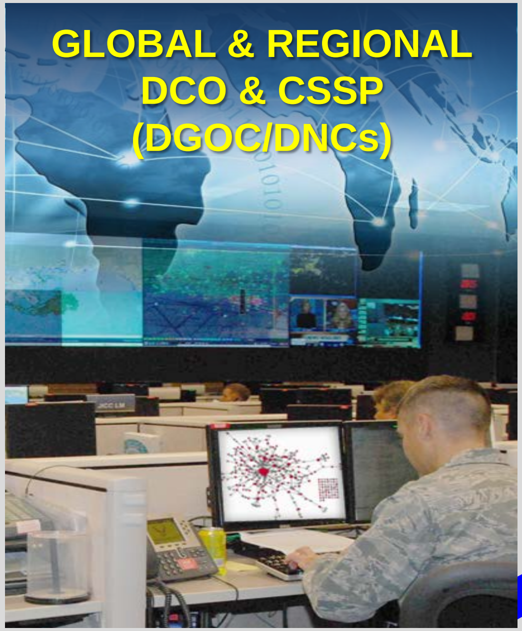
Chief, DISA Cyber Security Service Provider

Disclaimer

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.

DISA

Defensive Cyber Operations Across DISA



GLOBAL & REGIONAL DCO & CSSP (DGOC/DNCs)

- ▶ Monitor Persistent Presence
- ▶ Observe Suspicious Activity/ Sensor Data
- ▶ CSSP Execution
- ▶ Investigate Incident(s)
- ▶ Confirm Malicious Activity
- ▶ Report Incidents
- ▶ Cyber Threat Analysis

DEFENSIVE CYBER OPS DIVISION (HQS)

Current Operations

- ▶ Maintain SA for all defensive cyber operations
- ▶ Direct and Prioritize DCO
- ▶ Provide C2 for proactive cyber defense
- ▶ Determine/De-conflict Counter Measures
- ▶ Enterprise Cyber Threat Analysis

Plans, Strategy, Transformation

- ▶ DCO Strategy & Transformation
- ▶ DCO Requirements
- ▶ DCO-IDM Strategic/Deliberate/ Future Planning

CSSP

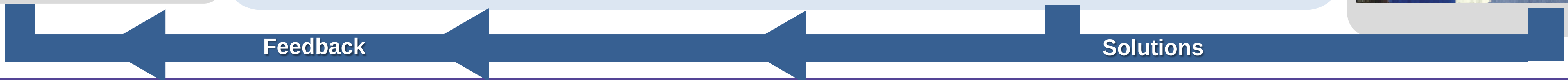
- ▶ CSSP Program Management
- ▶ Service Development
- ▶ Customer Engagement
- ▶ CSSP Compliance / Inspections

Mission Partners

DISA Internal Partners

DISA External Partners

PARTNERSHIPS + INNOVATIONS = SOLUTIONS



The Challenges

Data

- Big Data lakes are a drop in the ocean
- Escalating storage requirements will make PCAP storage cost prohibitive
- Break & Inspect increases volume of metadata and alerts

Strategy:

Advanced analytics

Software Defined Environment

Artificial Intelligence

Speed of Cyber

- Everyone loves fast internet, until they have to analyze it
- Alert Queuing & prioritization…not enough time to fully analyze all alerts
- By 2021, global fixed broadband speeds will reach 53 Mbps, up from 27.5 Mbps in 2016

Strategy:

Machine Learning

Auto Mitigation

DISA

The Challenges (continued)

Continued Trend toward Mobility

- 2018 World Population est. 7.6 billion
- # of Cellphone Users: 4.9 billion, # of Smartphone Users: 2.5 billion
- DoD microcosm: mobile device use doubled over last year

Strategy:

Industry partnerships for innovative and integrated perimeter, mid-tier and end-point solutions

The Cloud

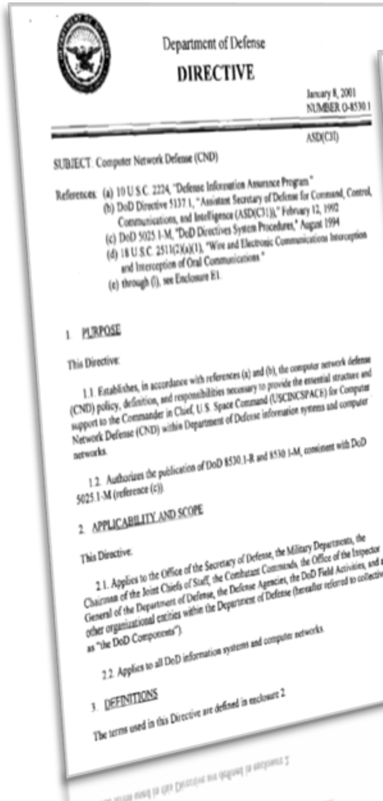
- Cloud defense is in a storming phase

Strategy:

Integrate Secure Cloud Computing Architecture into DCO environment to provide seamless cyber defense solution

Changes to DOD Policy

DoDD O-8530.1



Department of Defense

DIRECTIVE

January 8, 2001
NUMBER O-8530.1

ASD(C3I)

SUBJECT: Computer Network Defense (CND)

References: (a) 10 U.S.C. 2224, "Defense Information Assurance Program"
(b) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))," February 12, 1992
(c) DoD 5025.1-M, "DoD Directives System Procedures," August 1994
(d) 18 U.S.C. 2511(2)(a)(1), "Wire and Electronic Communications Interception and Interception of Oral Communications."
(e) through (l), see Enclosure E1.

1. PURPOSE

This Directive:

1.1. Establishes, in accordance with references (a) and (b), the computer network defense (CND) policy, definition, and responsibilities necessary to provide the essential structure and support to the Commander in Chief, U.S. Space Command (USCINCSPACE) for Computer Network Defense (CND) within Department of Defense information systems and computer networks.

1.2. Authorizes the publication of DoD 8530.1-R and 8530.1-M, consistent with DoD 5025.1-M (reference (c)).

2. APPLICABILITY AND SCOPE

This Directive:

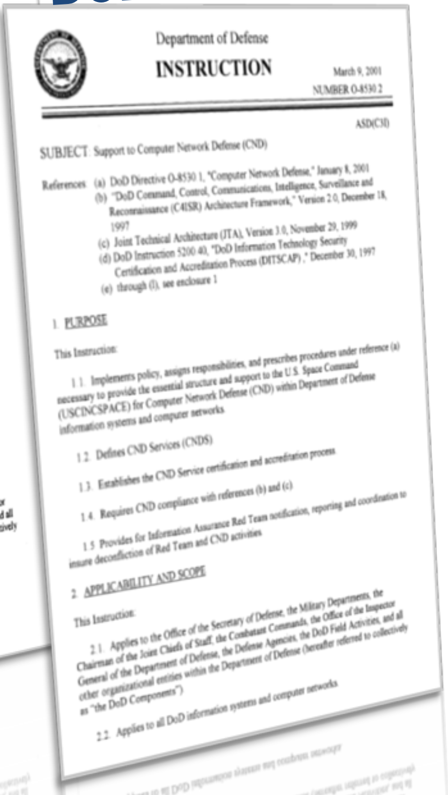
2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.2. Applies to all DoD information systems and computer networks.

3. DEFINITIONS

The terms used in this Directive are defined in enclosure 2

DoDI O-8530.2



Department of Defense

INSTRUCTION

March 9, 2001
NUMBER O-8530.2

ASD(C3I)

SUBJECT: Support to Computer Network Defense (CND)

References: (a) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001
(b) "DoD Command, Control, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) Architecture Framework," Version 2.0, December 18, 1997
(c) Joint Technical Architecture (JTA), Version 3.0, November 29, 1999
(d) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997
(e) through (l), see enclosure 1

1. PURPOSE

This Instruction:

1.1. Implements policy, assigns responsibilities, and prescribes procedures under reference (a) necessary to provide the essential structure and support to the U.S. Space Command (USCINCSPACE) for Computer Network Defense (CND) within Department of Defense information systems and computer networks.

1.2. Defines CND Services (CNDS).

1.3. Establishes the CND Service certification and accreditation process.

1.4. Requires CND compliance with references (b) and (c).

1.5 Provides for Information Assurance Red Team notification, reporting and coordination to insure deconfliction of Red Team and CND activities.

2. APPLICABILITY AND SCOPE

This Instruction:

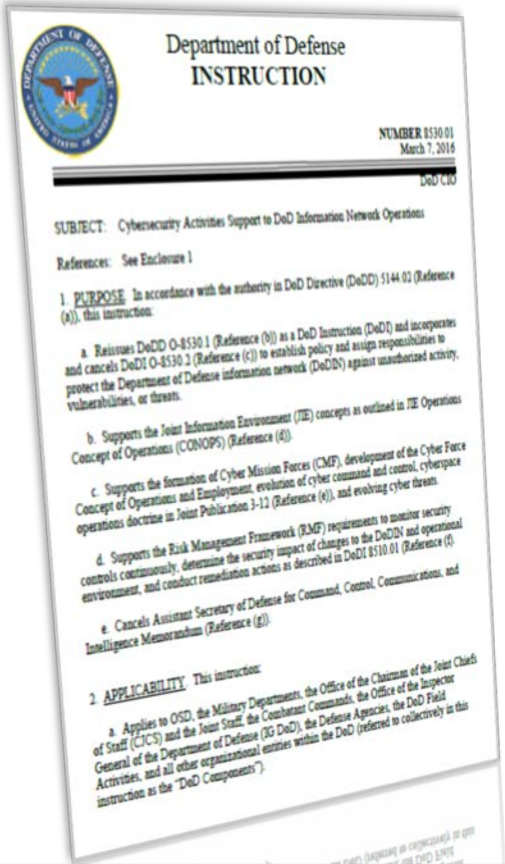
2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.2. Applies to all DoD information systems and computer networks.

2001

2016

DoDI 8530.01



Department of Defense

INSTRUCTION

NUMBER 8530.01
March 7, 2016

DoD CIO

SUBJECT: Cybersecurity Activities Support to DoD Information Network Operations

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)), this instruction:

a. Reissues DoDD O-8530.1 (Reference (b)) as a DoD Instruction (DoDI) and incorporates and cancels DoDI O-8530.2 (Reference (c)) to establish policy and assign responsibilities to protect the Department of Defense information network (DoDIN) against unauthorized activity, vulnerabilities, or threats.

b. Supports the Joint Information Environment (JIE) concepts as outlined in JIE Operations Concept of Operations (CONOPS) (Reference (d)).

c. Supports the formation of Cyber Mission Forces (CMF), development of the Cyber Force Concept of Operations and Employment, evolution of cyber command and control, cyberspace operations doctrine in Joint Publication 3-12 (Reference (e)), and evolving cyber threats.

d. Supports the Risk Management Framework (RMF) requirements to monitor security controls continuously, determine the security impact of changes to the DoDIN and operational environment, and conduct remediation actions as described in DoDI 8510.01 (Reference (f)).

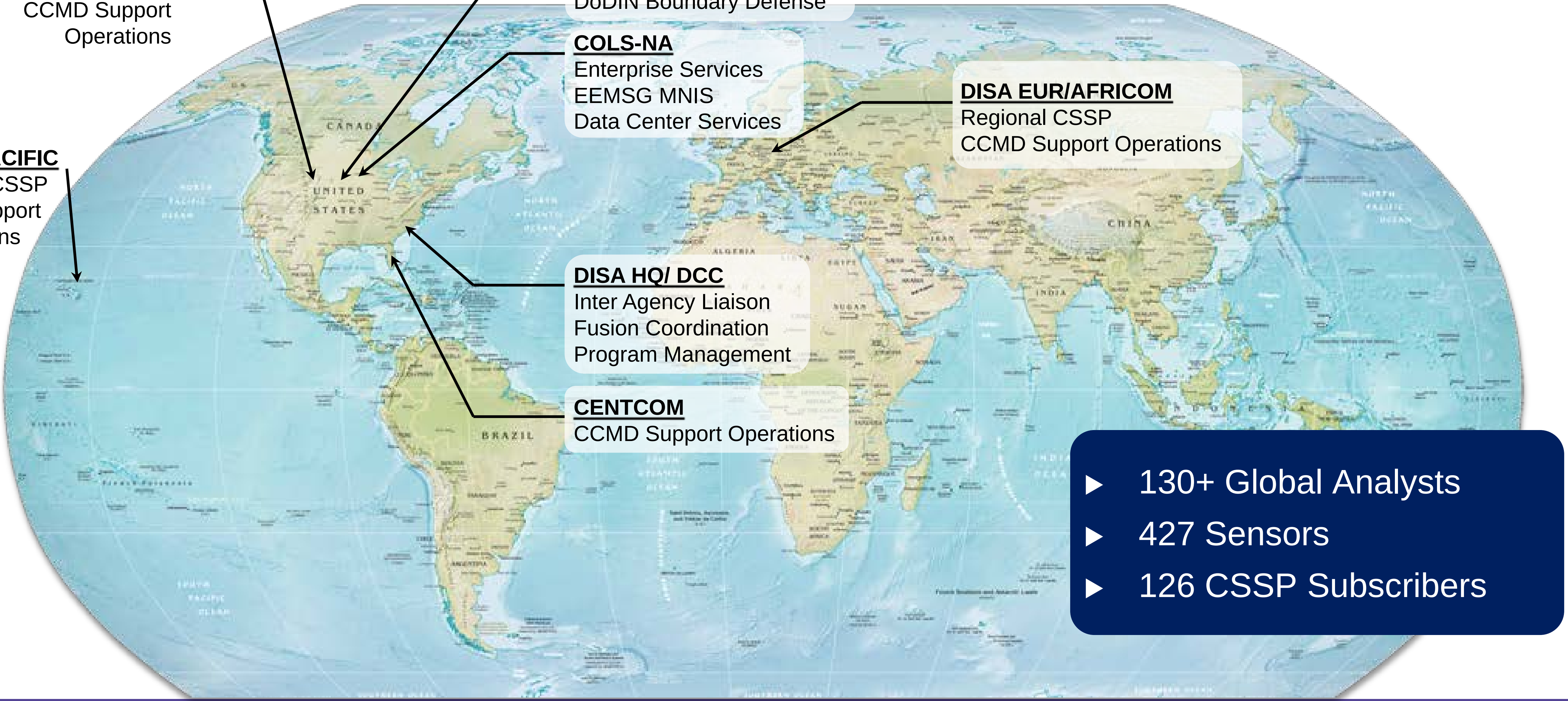
e. Cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum (Reference (g)).

2. APPLICABILITY. This instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

Current Policy: DoDI 8530.01,
"Cybersecurity Activities Support to DoD Information Network Operations"

DISA CSSP Global Support



NORTHCOM
CCMD Support
Operations

DISA PACIFIC
Regional CSSP
CCMD Support
Operations

GLOBAL
Regional CSSP
DoDIN Boundary Defense

COLS-NA
Enterprise Services
EEMSG MNIS
Data Center Services

DISA EUR/AFRICOM
Regional CSSP
CCMD Support Operations

DISA HQ/ DCC
Inter Agency Liaison
Fusion Coordination
Program Management

CENTCOM
CCMD Support Operations

- 130+ Global Analysts
- 427 Sensors
- 126 CSSP Subscribers

CSSP for Cloud: A Two-Phased Approach

PHASE 1
Initial Cloud CSSP Offering

Availability:

Now

Description:

Minimal CSSP services that can be provided to Commercial Cloud customers immediately. Provides limited monitoring capability utilizing existing sensors in the Cloud Access Point, Incident Reporting services, and technical support for implementing security in Cloud environments.

Applicability:

Information Impact Level 2/4/5;
IaaS/PaaS/SaaS

Benefit:

Allow CSSP customers to proceed with Cloud migration projects

Transitional Period of
Cloud CSSP Instantiation

Ongoing Development:

Description:

Integration and Investigation of key and essential data feeds from Cloud customer environments. Seeking to provide a more robust monitoring and analytic capability in pursuit of additional risk reduction capabilities in the Cloud environment.

Applicability:

Information Impact Level 2/4/5; IaaS

Benefit:

Development of more robust Cyber Security services to the evolving environment of the Commercial Cloud CSSP customer

PHASE 2
SCCA CSSP Offering

Availability:

Based on Secure Cloud Computing Architecture (SCCA) schedule

Description:

Perform sensing and correlation via centralized, common, DISA-managed enterprise Virtual Data Center Security Stack (VDSS) and Virtual Data Center Management Services (VDMs)

Applicability:

Information Impact Level 2/4/5; IaaS

Benefit:

Improve effectiveness and efficiency of incident detection and response through utilization of common sensor(s) for multiple Commercial Cloud CSSP customers

What We Need From Industry…

Tell us what you're doing

Partnerships – Key to our success!

Innovation, More Innovation, and Even More Innovation!

rate us

take the **3-question** survey
available on the AFCEA 365 app

visit us

DISA Booth # **443**

follow us

Facebook/USDISA

Twitter/USDISA

www.disa.mil

DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**