DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DISA CSSP Subscriber Services

Mr. David J. Nameroff
DISA CSSP Portfolio Manager

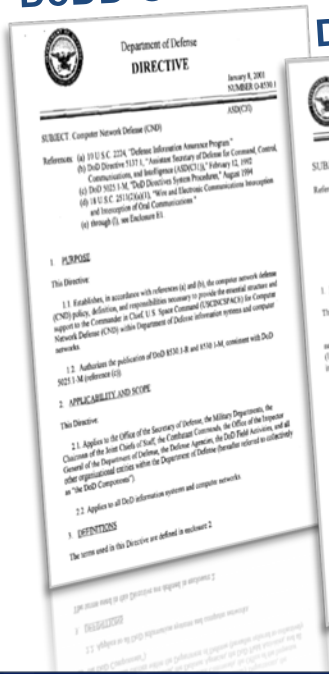
June 2017

Agenda

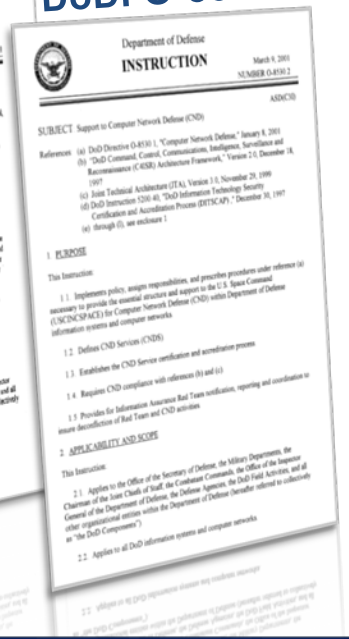
- **Changes in DoD Policy**
- **Traditional CSSP Services**
- **Future CSSP Services**
  - **Commercial Cloud**
  - **MilCloud**

Changes to DoD Policy

DoDD O-8530.1


Department of Defense
DIRECTIVE
January 8, 2001
SUBJECT: Computer Network Defense (CND)

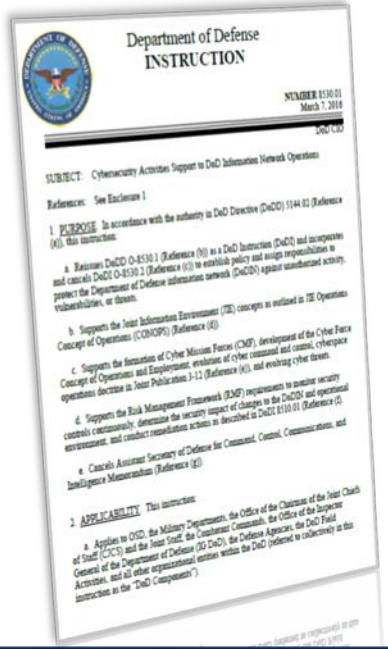
DoDI O-8530.2


Department of Defense
INSTRUCTION
March 9, 2001
SUBJECT: Support to Computer Network Defense (CND)

2001

2016

DoDI 8530.01


Department of Defense
INSTRUCTION
NUMBER 8530.01
March 7, 2016
SUBJECT: Cybersecurity Activities Support to DoD Information Network Operations

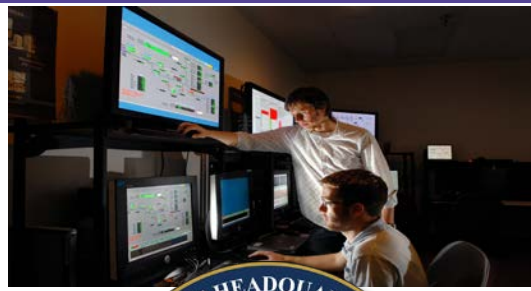
Current Policy: DoDI 8530.01,
"Cybersecurity Activities Support to DoD Information Network Operations"

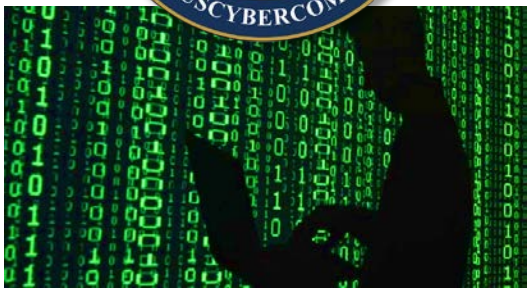
What Has Not Changed

- DoD Components are responsible for protection (secure and defend) of their portion of DoDIN
- Previous Computer Network Defense (CND) Service Providers remain certified and accredited as Cybersecurity (CS) Service Providers
- CSSPs (internal or external) support the DoD Component level
- Evaluator's Scoring Metrics (ESM) will continue to be used to evaluate service providers or internal organization capability to conduct cybersecurity activities

What Has Changed

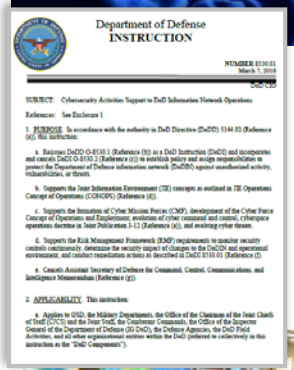
- **Establishes USSTRATCOM and USCYBERCOM responsibilities and authority (Directive Authority for Cyberspace Operations)**
- **Outlines Cybersecurity Activities conducted by DoD Components, their organizations, and individuals in Support of DoDIN Operations**
- **Requires individual services provided to external organizations be certified and accredited. These services will be offered through a formal agreement, Memorandum of Agreement (MOA), or fee-for-service**
- **Mandates service providers execute cybersecurity services (i.e., conduct cybersecurity activities) for external organizations with clearly defined service provider and system owner responsibilities**





What Will be Established or Maintained in Other Issuances

- **Service descriptions and CSSP accreditation process to provide services to external DoD Component organization(s) – (DoD Manual)**
- **Evaluation criteria for Service Provider or Internal Organization capability to provide cybersecurity in support of DoDIN operations – (DoD Manual)**
- **Command and Control (C2) Framework and Concept of Operations (CONOPS) for DoDIN Operations – (operation orders, operation plans, and execute orders relationships)**



Department of Defense
INSTRUCTION

NUMBER 8530.01
March 7, 2016

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.

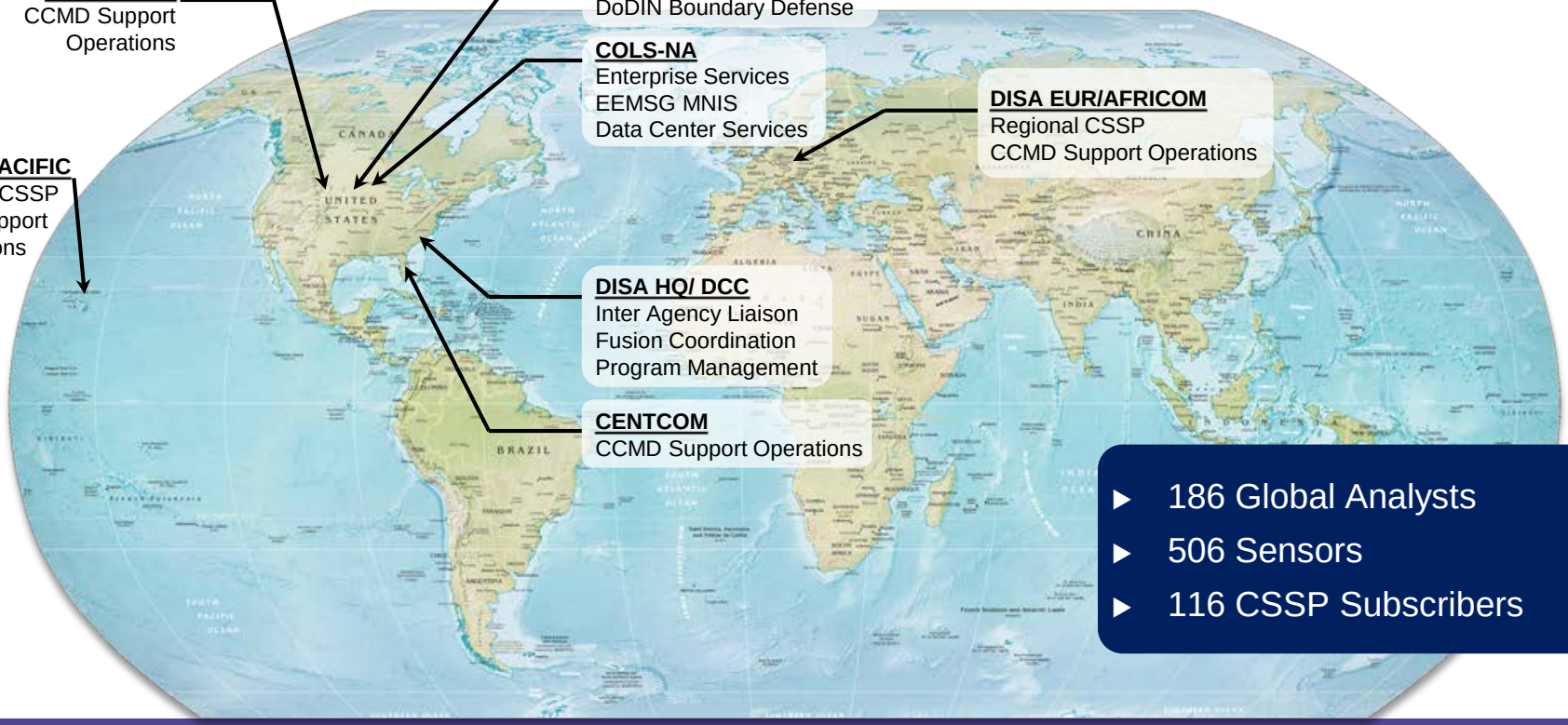
d. Supports the Risk Management Framework (RMF) requirements to monitor security controls continuously, determine the security impact of changes to the DoDIN and operational environment, and conduct remediation actions as described in DoDI 8510.01 (Reference (f)).

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").

DISA CSSP Global Support



- 186 Global Analysts
- 506 Sensors
- 116 CSSP Subscribers

CSSP for Cloud: Three-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

PHASE 2
Basic Cloud CSSP Offering

Availability:

October, 2017

Description:

Integrates feeds from Cloud customer environments to provide a more robust monitoring and analysis capability, and additional risk reduction capabilities to support the Cloud environment.

Applicability:

Information Impact Level 2/4/5; IaaS

Benefit:

Offer robust Cyber Security services to Commercial Cloud CSSP customers

PHASE 3
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

Available CSSP Services Summary

CSSP Offerings	Traditional CSSP	milCloud	milCloud+	Commercial Cloud (Initial)	Commercial Cloud (Basic, IaaS only)	Commercial Cloud (SCCA, IaaS only)
Availability:	**Now**	**June, 2017**	**June, 2017**	**Now**	**FY 18**	**TBD**
CSSP Subscription Services						
Malware Notification Protection (MNP)	☑	☑	☑		☑	☑
Support and Training (S&T)	☑	☑	☑	☑	☑	☑
INFOCON/CPCON	☑	☑	☑	☑	☑	☑
Information Assurance Vulnerability Management (IAVM)	☑	☑	☑	☑	☑	☑
Attack Sensing and Warning (ASW)	☑	☑	☑		☑	☑
Warning Intelligence (WI)	☑	☑	☑		☑	☑
Incident Reporting (IR)	☑	☑	☑	☑	☑	☑
Incident Handling Response (IHR)	☑	☑	☑			☑
Forensic Media Analysis (FMA)	☑	☑	☑			☑
Reverse Engineering/Malware Analysis (RE/MA)	☑	☑	☑	☑	☑	☑
Volatile Data Analysis (VDA)	☑	☑	☑			☑
Network Security Monitoring (NSM) Service	☑	☑	☑	CAP Only	☑	☑
Vulnerability Analysis & Assessment Support Services						
External Vulnerability Scans (EVS)	☑	☑	☑ (Optional)		☑	☑
Web Vulnerability Scans (WVS)	☑	☑	☑	☑ (Optional)	☑	☑
Penetration Testing (Pen Test)	☑ (Optional)	☑ (Optional)	☑ (Optional)		☑ (Optional)	☑ (Optional)
Red Team Operations (RTO)	☑ (Optional)	☑ (Optional)	☑ (Optional)		☑ (Optional)	☑ (Optional)
Intrusion Assessment	☑ (Optional)	☑ (Optional)	☑ (Optional)		☑ (Optional)	☑ (Optional)
Sensor Sustainment Services						
Sensor Sustainment & Configuration Management	☑	☑ (one-time fee)	☑ (one-time fee)	☑ (one-time fee)	☑	☑

CSSP Services/Roles and Responsibilities

Detailed on DISA's CSSP website at
https://disa.deps.mil/ext/cop/cdsp/SitePages/CDSPHome.aspx

Helpful Resources

STIGs	
STIGs Homepage	http://iase.disa.mil/stigs/Pages/index.aspx
STIGs Mailing List	http://iaseapp.disa.mil/stigs/script/subscribe.aspx

Cloud	
DISA Cloud Homepage	http://iase.disa.mil/cloud_security/Pages/index.aspx

milCloud	
milCloud Homepage	https://milcloud.mil
Customer Support	https://community.forge.mil//group/milcloud-customer-support

CSSP Subscriber Services	
All inquiries	disa.letterkenny.re.list.cdsp-requests@mail.mil

rate us

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

visit us

DISA Booth # 443

follow us

Facebook/USDISA

Twitter/USDISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

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

Services Overview

Service Name	Services Provided	Type
Malware Notification Protection (MNP)	- Management through DISA's HBSS (not part a DISA CSSP service offering) program, accomplished via polling the ePO. DISA CSSP leverages DISA Component's HBSS program and serves as a facilitator for MNP to CSSP Subscribers through the Component's program - Warnings and updated information malicious threats provided through reports (i.e. Situational Awareness Reports, ARs, Daily summary) - Access to 24x7 support for virus responses and self-reporting	Required
Subscriber Support & IA Training (S&T)	- Assistance with identifying Cybersecurity training requirements, upon request. - Access to Cybersecurity Computer Based Training (CBT) and classroom classes at https://disa.deps.mil/ext/cop/iase/classroom_training/Pages/index.aspx and http://iase.disa.mil/eta/Pages/online-catalog.aspx	Required
INFOCON Compliance/NetOps Awareness (INFOCON)	- Monitor the CSSP Subscriber's INFOCON/CPCON level - Track and Report INFOCON/CPCON compliance to USCYBERCOM - Guidance and assistance as required/requested	Required
Information Assurance Vulnerability Management (IAVM)	- Notification of IAVM guidance, assistance, and facilitation of communication to IAVM SMEs as required/requested - Task Orders, FRAGOS, NTOC Reports, Situational Awareness Reports, Defensive Cyber Operations Metrics Report	Required

Services Overview - Continued

Service Name	Services Provided	Type
Network Security Monitoring/Intrusion Detection	- Monitoring of Unclassified and Classified network Command Communication Service Designator (CCSDs)/IPs using approved sensors via the assigned DISA DNC - Various reports such as Cat 3 Report, Cat 6 Report (on request only basis), Trend Analysis Reports	Required
Attack Sensing & Warning (ASW)	- Notification of suspicious/malicious network traffic or potential computer attacks - Upon identification, analysis of low-level ("low and slow") events to identify unauthorized activity utilizing exploratory problem-solving or self-learning techniques - Orders (Task Orders, FRAGOS, NTOC Reports). - Situational Awareness Reports - Daily Report - Detect/Warning Intelligence. - Defensive Cyber Operations Metrics Report	Required
Warning Intelligence	Notification of suspicious/malicious network traffic or potential computer attacks via Situational Awareness Reports (SARs) and Fusion Reports - Develop and distribute countermeasures or guidance to prevent or mitigate potential cyber event impacts	Required

Services Overview - Continued

Service Name	Services Provided	Type
Incident Reporting	-- Reporting incidents into Joint Incident Management System (JIMS)	Required
Incident Response Support	-Provide offsite Volatile Data Analysis (VDA), Forensic Media Analysis (FMA), and Reverse Engineering/Malware Analysis (RE/MA) support as requested or required. Depending on the type of support this can include acknowledgement of the request, appropriate updates, and reports as defined	Required
Incident Handling Response (IHR)	-One on-site Intrusion Assessment or Incident Response as requested or required via the DISA Incident Response and Recovery Team (IRRT) -Updated incident response guidelines, checklists and recommended procedures at least annually	Required
Sensor Sustainment & Configuration Management	-Ensure service are delivered -Efforts to validate service is delivered at an acceptable level of quality -SLA is maintained and understood -Configure, patch, maintain sensors where applicable	Required
Annual Renewal of Sensor Maintenance and Licensing (AL/SML)	-Maintain and keep current vendor maintenance, support, and licensing throughout the sensor lifecycle	Required

DISA Cyber Security Contacts

DISA Risk Management Executive (RE) - Letterkenny, PA
For questions about support agreements or general questions:
disa.letterkenny.re.list.cdsp-requests@mail.mil
FSOCSSPRequests@disa.smil.mil (SIPR)

DISA CSSP Subscriber Outreach Distro
disa.letterkenny.ce.list.cssp-subscriber-outreach@mail.mil

DISA Command Center (DCC) - Ft. Meade, MD
disa.meade.ops.mbx.dcc-nawo@mail.mil
disa.meade.ops.mbx.dcc-nawo@mail.smil.mil (SIPR)
Phone: (301) 225-3508

DISA Global Operations Command Net Assurance - Scott AFB
disa.scott.conus.mbx.noc-gnsc-netassurance-nawo@mail.mil
disa.scott.conus.mbx.gnsc-netassurance@mail.smil.mil (SIPR)
Phone: (618) 220-9032
DSN 770-9032

Columbus Net Assurance (COL-NA) - Columbus, OH
disa.columbus.eis.mbx.cols-esdna@mail.mil
disa.columbus.esc.mbx.esdna@mail.smil.mil (SIPR)
Phone: (614) 692-5600/3291
DSN 850-5600/3291

DISA NetOps Center Europe (DNC-EUR) - Stuttgart, GE
disa.stuttgart.eu.mbx.net-assurance@mail.mil
disa.stuttgart.eu.mbx.net-assurance@mail.smil.mil (SIPR)
Phone: 011 49 711 686 395413
DSN 314 434-5413

DISA NetOps Center Pacific (DNC-PAC) - Oahu, HI
disa.jbphh.pac.mbx.dnc-net-assurance@mail.mil
disa.jbphh.pac.mbx.dnc-net-assurance@mail.smil.mil (SIPR)
Phone: (808) 472-4000, option 5
DSN 315 472-4000, option 5