DISA

DISA Cybersecurity Service Provider (CSSP)

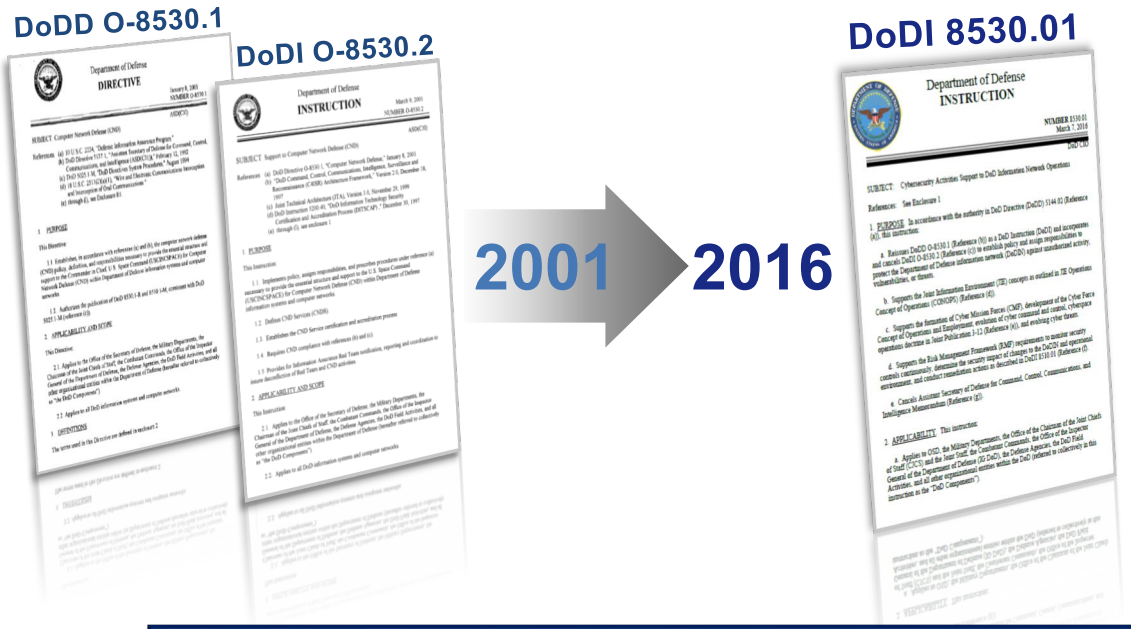
Mission Partner Brief

Mr. Darrell Fountain
Chief, DISA CSSP Services Branch
November 2018

Agenda

- Changes to DOD Policy
- CSSP Mission
- Customer Assessment & Onboarding Process
- CSSP Services
- Program Initiatives

Changes to DOD Policy



Requires that:

DoD-owned or DoD-controlled information systems… be aligned to…supporting cybersecurity service provider(s)… which will provide required cybersecurity service to aligned systems."

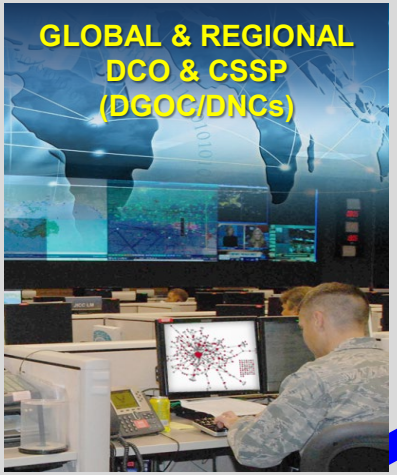
DoDI 8530.01,
"Cybersecurity Activities Support to DoD Information Network Operations"

DISA CSSP MISSION

- Provide CSSP services for DISA Enterprise, Combatant Commands (CCMDs), DoD agencies, and Cleared Defense Contractors (CDCs) that subscribe and align to DISA
- Perform defensive operations by monitoring and providing situational awareness for identified portions of the CONUS and inter-theater Enterprise Infrastructure backbone
- Monitor subscriber boundary, theater, and global incidents; leveraging strategic end to end analysis to provide Cyber Security recommendations
- Assist CCMDs, DoD Agencies, DISA-sponsored Defense Contractors, Federally Funded Research and Development Contractors (FFRDCs) and mission partners to defend their networks

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 (DCO)
- ▶ 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

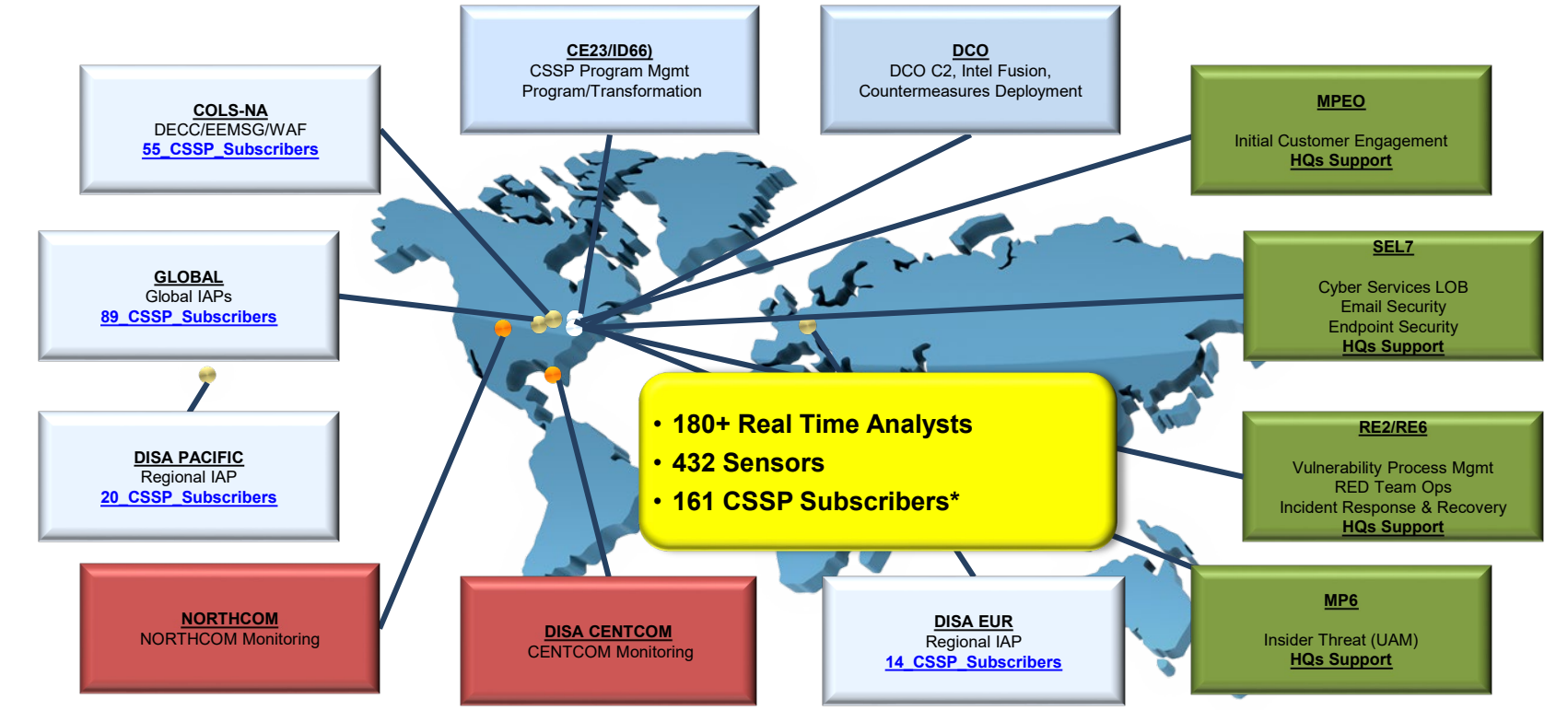
DISA External Partners

PARTNERSHIPS + INNOVATIONS = SOLUTIONS

Feedback

Solutions

GEOGRAPHIC CONTEXT



*CSSP Subscribers Are Supported By Multiple Organizations Across the Agency

Current CSSP Services Construct

Traditional

- CSSP service designed to protect against, defend, and respond to suspicious or malicious cyber activity associated with network traffic leveraging a Mission Partner's Command Communications Service Designator(s) (CCSD) where IT assets and supporting infrastructure reside at a Base, Camp, Post, or Station (BCPS).

milCloud/milCloud+

- CSSP service designed to protect against, defend and respond to suspicious or malicious cyber activity associated with network traffic entering or exiting the unique Virtual Data Center(s) (VDC) hosted within DISA DataCenter utilizing the Datacenter network infrastructure. Please note that Mission Partner CSSP Alignment to DISA cannot be assumed through DISA Datacenter Hosting.

Commercial Cloud

- CSSP service designed to protect against, defend, and respond to suspicious or malicious cyber activity associated with network traffic entering or exiting the Mission Owner's (MO) Virtual Private Cloud (VPC) Secure Cloud Computing architecture (SCCA) (pending) defense for Impact Level 4 and 5 traffic traversing Boundary Cloud Access Point (BCAP). MP information is hosted in a commercially-owned infrastructure (Amazon AWS, MS Office 365, MS Azure, Oracle, etc...)

Traditionally Hosted Datacenter Program (THDP)

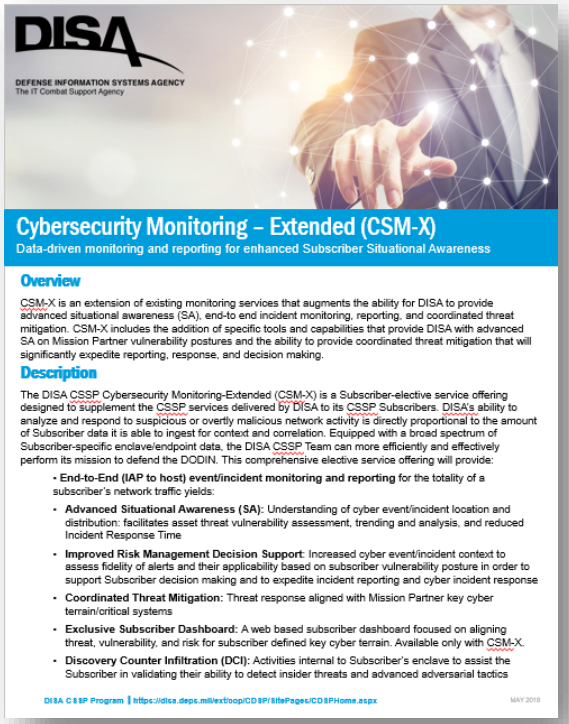
- CSSP service designed to protect against, defend, and respond to suspicious or malicious cyber activity associated with network traffic entering or exiting the unique Operating/Virtual Environment(s) of a DISA Datacenter-Hosted Mission Partner utilizing the Datacenter network infrastructure (excludes floorspace-only MPs). Please note that Mission Partner CSSP Alignment to DISA cannot be assumed through DISA Datacenter Hosting

Complete service descriptions and additional information available at: https://disa.deps.mil/ext/cop/cdsp/SitePages/CDSPHome.aspx

Overview of Cybersecurity Monitoring – Extended

Cybersecurity Monitoring – Extended (CSM-X) is an extension of existing monitoring services that augments the ability for DISA to provide advanced situational awareness (SA), end-to end incident monitoring, reporting, and coordinated threat mitigation. CSM-X includes the addition of specific tools and capabilities that provide DISA with advanced SA on Mission Partner security posture and the ability to provide coordinated threat mitigation.

- Advanced Situational Awareness (SA)
- Improved Cybersecurity Decision Support
- Coordinated Threat Mitigation
- Subscriber-Specific Dashboard
- Superior Discovery Counter Infiltration (DCI) Activities



DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Cybersecurity Monitoring – Extended (CSM-X)

Data-driven monitoring and reporting for enhanced Subscriber Situational Awareness

Overview

CSM-X is an extension of existing monitoring services that augments the ability for DISA to provide advanced situational awareness (SA), end-to end incident monitoring, reporting, and coordinated threat mitigation. CSM-X includes the addition of specific tools and capabilities that provide DISA with advanced SA on Mission Partner vulnerability postures and the ability to provide coordinated threat mitigation that will significantly expedite reporting, response, and decision making.

Description

The DISA CSSP Cybersecurity Monitoring-Extended (CSM-X) is a Subscriber-elective service offering designed to supplement the CSSP services delivered by DISA to its CSSP Subscribers. DISA's ability to analyze and respond to suspicious or overtly malicious network activity is directly proportional to the amount of Subscriber data it is able to ingest for context and correlation. Equipped with a broad spectrum of Subscriber-specific enclave/endpoint data, the DISA CSSP Team can more efficiently and effectively perform its mission to defend the DODIN. This comprehensive elective service offering will provide:

- **End-to-End (IAP to host) event/incident monitoring and reporting** for the totality of a subscriber's network traffic yields:
  - **Advanced Situational Awareness (SA)**: Understanding of cyber event/incident location and distribution: facilitates asset threat vulnerability assessment, trending and analysis, and reduced Incident Response Time
  - **Improved Risk Management Decision Support**: Increased cyber event/incident context to assess fidelity of alerts and their applicability based on subscriber vulnerability posture in order to support Subscriber decision making and to expedite incident reporting and cyber incident response
  - **Coordinated Threat Mitigation**: Threat response aligned with Mission Partner key cyber terrain/critical systems
  - **Exclusive Subscriber Dashboard**: A web based subscriber dashboard focused on aligning threat, vulnerability, and risk for subscriber defined key cyber terrain. Available only with CSM-X.
  - **Discovery Counter Infiltration (DCI)**: Activities internal to Subscriber's enclave to assist the Subscriber in validating their ability to detect insider threats and advanced adversarial tactics

DISA C S P Program | https://disa.deps.mil/ext/cop/CDSP/SitePages/CDSPHome.aspx MAY 2018

Overview of JRSS Enabled CSSP Services

Cybersecurity Service Provider – JRSS Enabled (CSSP-J)

- CSSP service designed to protect against, defend, and respond to suspicious or malicious cyber activity associated with network traffic for mission partners who connected to the Joint Regional Security Stack (JRSS) architecture.

Cybersecurity Monitoring JRSS (CSM-J)

- Included with the CSSP-J services package is CSM-J, a unique set of additional cybersecurity support that is only available to JRSS subscribers as part of the CSSP-J service offering. CSM-J leverages the suite of cybersecurity capabilities/devices included with the JRSS to allow the DISA CSSP to provide the additional support outlined below:

    - Intrusion Prevention
    - Network Anti-Malware
    - Data Loss Detection and Alerting
    - Network Anomalous Traffic Analysis


DISA

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Cybersecurity Service Provider – JRSS (CSSP-J)

JRSS Enabled CSSP services that include exclusive CSM-J activities

Overview

The JRSS-Enabled CSSP Service offering is designed for DISA CSSP Subscribers that have connected to the Joint Regional Security Stack (JRSS) architecture, either through new connections or migration from their traditional enclave CSSP sensing constructs. These subscribers benefit from a suite of cybersecurity capabilities that enhance the ability of DISA CSSP to more comprehensively Detect, and Respond to suspicious or overtly malicious cyber activity on behalf of its Subscribers.

The JRSS-Enabled CSSP Service Offering is comprised of 5 of the 7 cybersecurity activities that align with the regulatory requirements prescribed in DODI 8530.01. Those services include:

- **Warning Intelligence (WI) and Attack Sensing and Warning (AS&W)**
- **Malware Protection**
- **Cyber Incident Handling**
- **Vulnerability Assessment and Analysis (VAA)**
- **Vulnerability Management**

Cybersecurity Monitoring JRSS – (CSM-J)

Included with the CSSP-J services package is CSM-J, a unique set of additional cybersecurity support that is only available to JRSS subscribers as part of the CSSP-J service offering. CSM-J leverages the suite of cybersecurity capabilities/devices included with the JRSS to allow the DISA CSSP to provide the additional support outlined below:

- **Intrusion Prevention**
- **Network Anti-Malware**
- **Data Loss Detection and Alerting**
- **Network Traffic Analysis**

Continuous Monitoring and DODIN User Activity Monitoring (UAM) are not currently included as part of the DISA CSSP Service Offering. The JRSS-enabled CSSP services are detailed in the following section. This section also defines DISA and Subscriber Roles and Responsibilities for each activity.

DISA CSSP Program | https://disa.depe.mil/extd/oop/CDSP/SitePages/CDSPHome.aspx

CSSP On-boarding Process Overview

REQUEST INITIATION

- Mission Partner initiates request through MPEO
- Completed Service Request Form (SRF) and network diagram are returned to MPEO and request is forwarded to CSSP Team

SERVICE PLANNING

- Submission reviewed and Secure Architecture Review complete
- Letter Estimate Provided to Mission Partner
- Mission Partner reviews/accepts LE and funds effort

SERVICE IMPLEMENTATION

- Mission Partner procures sensors and configuration/installation is completed **(N/A for THDP, Milcloud, Commercial Cloud)**
- Data configuration/operational testing complete

SERVICE ACTIVATION

- SLA prepared and alignment achieved

All requests to obtain CSSP Services must be submitted by sending an email to disa.meade.bd.mbx.bdm4-mpeo-support@mail.mil

DISA CSSP TEAM KEY INITIATIVES

- **Supporting CSSP Transformation**
- **Exploring expanded DISA CSSP Support**
- **Supporting DoD CIO regulation revision/rewrite (DoD 8530.01-M)**
- **Managing 160+ customers**
    - Executing CSSP onboarding process
    - Producing security architecture reviews
    - Facilitating agreement reviews and maintenance of customer security services

How To Order

To obtain CSSP Services an email should be sent to the Mission Partner Engagement Office (MPEO)

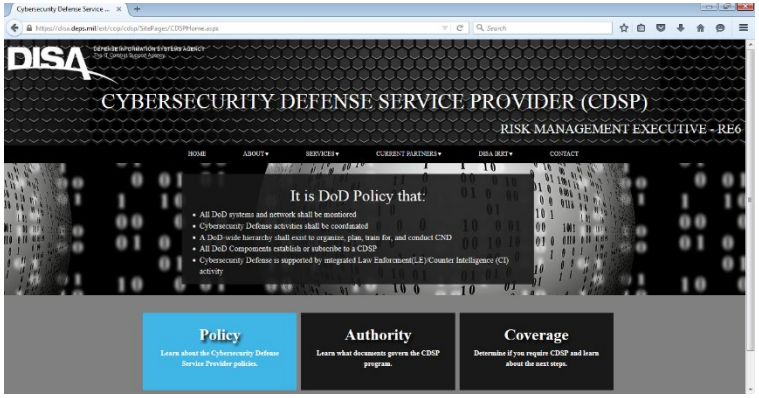
disa.meade.bd.mbx.bdm4-mpeo-support@mail.mil

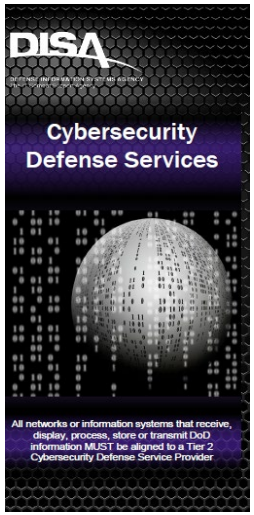
Need to speak to a subject matter expert? Please send an email to:
Disa.Letterkenny.re.list.cdsp-requests@mail.mil

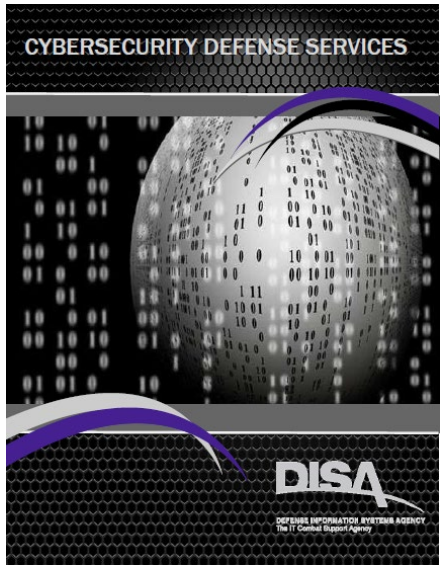
DISA Cybersecurity Service Provider Information Portal:
https://disa.deps.mil/ext/cop/cdsp/SitePages/CDSPHome.aspx

CSSP INFORMATION PORTAL

Brochures
Contact Information
Service Descriptions
Roles & Responsibilities
Resources
https://disa.deps.mil/ext/cop/cdsp/SitePages/CDSPHome.aspx







DISA CSSP Program Contact Information

Contact Information:

Customer Support:
717-267-4260
717-267-8076

DISA Cybersecurity Service Provider Information Portal:
https://disa.deps.mil/ext/cop/cdsp/SitePages/CDSPHome.aspx

DEFENSE INFORMATION SYSTEMS AGENCY

The IT Combat Support Agency

UNITED IN SERVICE TO OUR NATION