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

**DoD-owned or DoD-controlled information systems... be aligned to... supporting cybersecurity service provider(s)... which will provide required cybersecurity service to aligned systems.**
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
Globally and Regionally:
DCO & CSSP
(DGOC/DNCs)

Defensive Cyber Operations 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

Trust in DISA: Mission First, People Always!
GEOGRAPHIC CONTEXT

*CSSP Subscribers Are Supported By Multiple Organizations Across the Agency

- 180+ Real Time Analysts
- 432 Sensors
- 161 CSSP Subscribers*

• COL 5-NA
  DECC/EEMS/GWAF
  55_CSSP_Subscribers

• GLOBAL
  Global IAPs
  89_CSSP_Subscribers

• DISA PACIFIC
  Regional IAP
  20_CSSP_Subscribers

• NORTHCOM
  NORTHCOM Monitoring

• DISA CENTCOM
  CENTCOM Monitoring

• DCO
  DCO C2, Intel Fusion, Countermeasures Deployment

• MPEO
  Initial Customer Engagement
  HQs Support

• SEL7
  Cyber Services LOB
  Email Security
  Endpoint Security
  HQs Support

• RE2/RE6
  Vulnerability Process Mgmt
  RED Team Ops
  Incident Response & Recovery
  HQs Support

• MP6
  Insider Threat (UAM)
  HQs Support

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

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

DISA Cybersecurity Service Provider Information Portal: