C2 of DISA’s Enterprise

Mr. Scott Rodakowski
Center for Operations, DISA
"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 United 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."
DISA’s Enterprise Infrastructure and Services

Robust, diverse, resilient, and protected communications and computing environment enabling warfighting operations

CLOUD SERVICES
UNCLASSIFIED
UNITED IN SERVICE TO OUR NATION

**DEFEND**
Command & Control (C2)
- 1,400 MIl, 5,600 CIV and 8,000 Contractors in 18 States, 8 Countries
- ~11.3B Budget

**OPERATE**
- DISA Provides, Operates and Assures:
  - $24B Enterprise, 11 Core Data Centers
  - >1000 Enterprise Apps, Worldwide Transport
  - >500 Teleport Missions, >50 RPA Flights

**COMMAND & CONTROL (C2)**
- Events requiring Orders:
  - Exercises
  - Operations
  - CPT Employment

**INCIDENTS**
- >10M Alarms
- ≥24 Critical Auth SVC Interruptions
- >2400 Trouble Calls

**EVENTS**
- >10M Alarms
- ≥24 Critical Auth SVC Interruptions
- >2400 Trouble Calls

**COMPLIANCE MONITORING**
- 45 Orders Tracked

**DOD EVENTS / day**
- >500 Sensors
- >798M Events
- >300M Blocks

**DCO Incidents / day**
- >36 Cybersecurity incidents
- >14 Phishing Attacks
- >80% Emails Blocked

**DOD’s Cyber Forward Edge of the Battle Area**
- 3M+ Users Defended
- 102 CDSP Customers
- 300 TB of Data/38M E-mails Processed

**OUR GOAL**
= 100% Mission Assurance
Full Spectrum Operations

Operation Gladiator Shield
Global Cyber

Ukraine Engagement
USEUCOM

Operation United Assistance
Jukebox Lotus / Juniper Micron / Juniper Nimbus
USAFRICOM

Operation Freedom Sentinel
Afghanistan
USCENTCOM

Homeland Defense
Drug Interdiction
USNORTHCOM / USOUTHCOM

Disaster Relief
Nepal
USPACOM

Inherent Resolve
Iraq/Syria
USCENTCOM
DISA Network Operations Global Command and Control

- **C2** of DISA’s Global Infrastructure and Services
- Provide support and services to the National Military Command Center
- 24x7 GCCS-J Tier I/II service support

- **24x7** Operations for DISA and mission partner applications
- Cyber Security & Maintenance of DISA’s computing environment

- **C2** & Support
  - Network Services/Transport/DCO
  - Computing/Enterprise Services
  - Field Office

- **LEGEND:**
  - DISA NetOps Center (DNC)
  - Joint Staff Support Center (JSSC)
  - White House Communications Agency (WHCA)
  - DISA Global Operations Command (DGOC)
  - DISA Center for Operations (DCC)
  - DECC Oklahoma City
  - DECC Ogden
  - DISA-NORTHCOM
  - DISA STRATCOM
  - DISA AFIRCOM
  - DISA TRANSCOM
  - DISA STRATCOM
  - DISA CENTERCOM
  - DISA SOUTHCOM
  - DISA Field Office

- **Unclassified**
C2 of DODIN OPS, DCO-IDM & JIE
Unity of Command and Unity of Effort

The DISA Enterprise

The DISA Enterprise
- Enterprise Applications
- Enterprise Infrastructure
- Enterprise Foundational Services
- SMC
- Global Service Desk
- DNC CONUS/PAC

Catalyst for Change:
- Delivery of Enterprise Services
- Core Data Center & Shared IT Infrastructure
- Single Security Architecture
- EOC Maturity

Benefits of Change:
- Enhanced Mission Effectiveness
- Defensible Cyber Terrain
- Resource & Personnel Efficiencies
- Operational Responsiveness

UseUcom

USCYBERCOM

JFHQ DoDIN GEOC

- Plan
- Monitor
- Assess

- Synchronize
- Coordinate
- De-conflict

DODIN Command

Disa NetOps Center

Enterprise Operations Center

D-CPT

Theater Service Operations

Usafrcicom

Joint Force Cyber Component Command

C-CPT

Disa Operations

Priorities & Direction

Priorities & Synchronization

Tasking & Synchronization

Priorities & Direction

Priorities & Synchronization

Integrated Tasking Authority

- Incidents
- Triage
- Categorization

- Escalation
- Resolution
- Reporting

Disa Enabled Missions

Disa Users

119 Theater Service Desk
Day in the Life of DECC Ogden

**Operate**
- DISA DECC Ogden Operates IT Systems hosting Mission Partner Applications for 3.5 M Users
  - Fully ITIL Compliant
- 200 Managed Operating Environments
  - 42 z/OS Partitions
  - 2.9 PB Managed Storage
  - 45000 System Backups/week
  - 500,000 Batch jobs/week
- 3 Operational turnovers/day
  - 5500 Incidents/week
  - 320 Change Requests/week
  - 10 Maintenance Windows/month

**Command**
- DLA Enterprise Business System, $1,200,000,000 transactions processed annually
- USTRANSCOM Defense Personal Property System, 555,000 Shipments/Year
- Wide Area Workflow, $1,500,000,000 invoices/day

**Defend**
- Fully Secure Enterprise Class Data Center Located on Hill AFB, Utah
- Weekly ACAS Scans
- Monthly SRG Compliance Checks
- Yearly AT 801 Audit
- Physical Security
- Personnel Security
- 24X7X365 Operations

**Events**
- 2000 Managed Operating Environments
- 42 z/OS Partitions
- 2.9 PB Managed Storage
- 45000 System Backups/week
- 500,000 Batch jobs/week

**Incidents**
- 3 Operational turnovers/day
- 5500 Incidents/week
- 320 Change Requests/week
- 10 Maintenance Windows/month

**Actions**
- 24X7X365 Operations
- Fully Secure Enterprise Class Data Center Located on Hill AFB, Utah
- Weekly ACAS Scans
- Monthly SRG Compliance Checks
- Yearly AT 801 Audit
- Physical Security
- Personnel Security
- 24X7X365 Operations

Remotely Manage Systems at 7 sites, DWCF Funded
Securing Mission Partner Information Systems

- **DoD Policy/Defensive Operations**
  - DoDI 8500.1 – Cybersecurity
  - DoDI 8510.01 – Risk Management Framework (RMF)
  - US Cyber Command Orders and Directives (OPORDS/TASKORDS/FRAGOS)
  - JFHQ-DODIN/ DISA Headquarters Orders and Directives (TASKORD)

- **Assessment and Authorization (Formerly Certification and Accreditation)**
  - Risk Management Framework (RMF) – Replaced DIACAP as the process to perform risk analysis of an application or network enclave to grant an Authority to Operate (ATO).

- **Automated Cybersecurity Tools**
  - Host Based Security Systems (HBSS) – Suite of McAfee applications running on Windows/UNIX/Linux systems providing firewall, antivirus, rogue system detection, intrusion detection, and vulnerability compliance.
  - Assured Compliance Assessment Solution (ACAS) - Tenable network scanner running weekly and ad hoc credentialed compliance scans across Windows/UNIX/Linux systems.
  - BladeLogic – BMC tool used to deploy Windows/UNIX/Linux vendor patches and run weekly compliance scans.

- **Continuous Monitoring Risk Scoring (CMRS)**
  - DoD database system used to track cybersecurity compliance and determine risk. Automatic data feeds from HBSS and ACAS are rolled up to this system. Risk algorithms are used to calculate and a risk score (A, B, C, D, or F) by agency, directorate, or application.

- **Manual Compliance Checks**
  - Security Requirements Guides (SRG)/Security Technical Implementation Guide (STIG) – These guides are developed to provide in-depth hardening requirements for operating systems, network devices, applications, databases, and web servers.