



Joint Tactical Data Link Lab



Mission:

Provide interoperability test, assessment, and certification support for the DoD National Security Systems/Information Technology Systems (NSS/ITS).



- **Capabilities:**

- Provides DOD the capability to perform joint and combined C4I system tactical data link interoperability testing
 - LINK 11
 - LINK 11B
 - LINK 16
- Test execution and post-test data analysis
- Comprehensive data base of all test results



- **Major Test Equipment**

- **Joint Interoperability Modular Evaluation System (JIMES) Server, Intel Platform** 1
- **JIMES Workstations, Intel Platform** 4
- **Theater Air and Missile Defense (TAMD) Interoperability Assessment Capability (TIAC), Remote Gateway, Intel Platform** 1
- **SPAWAR Gateway Term, OS2 Platform** 5
- **Multi-Link System Training Tool (MLST3) Workstation, Intel Platform** 4

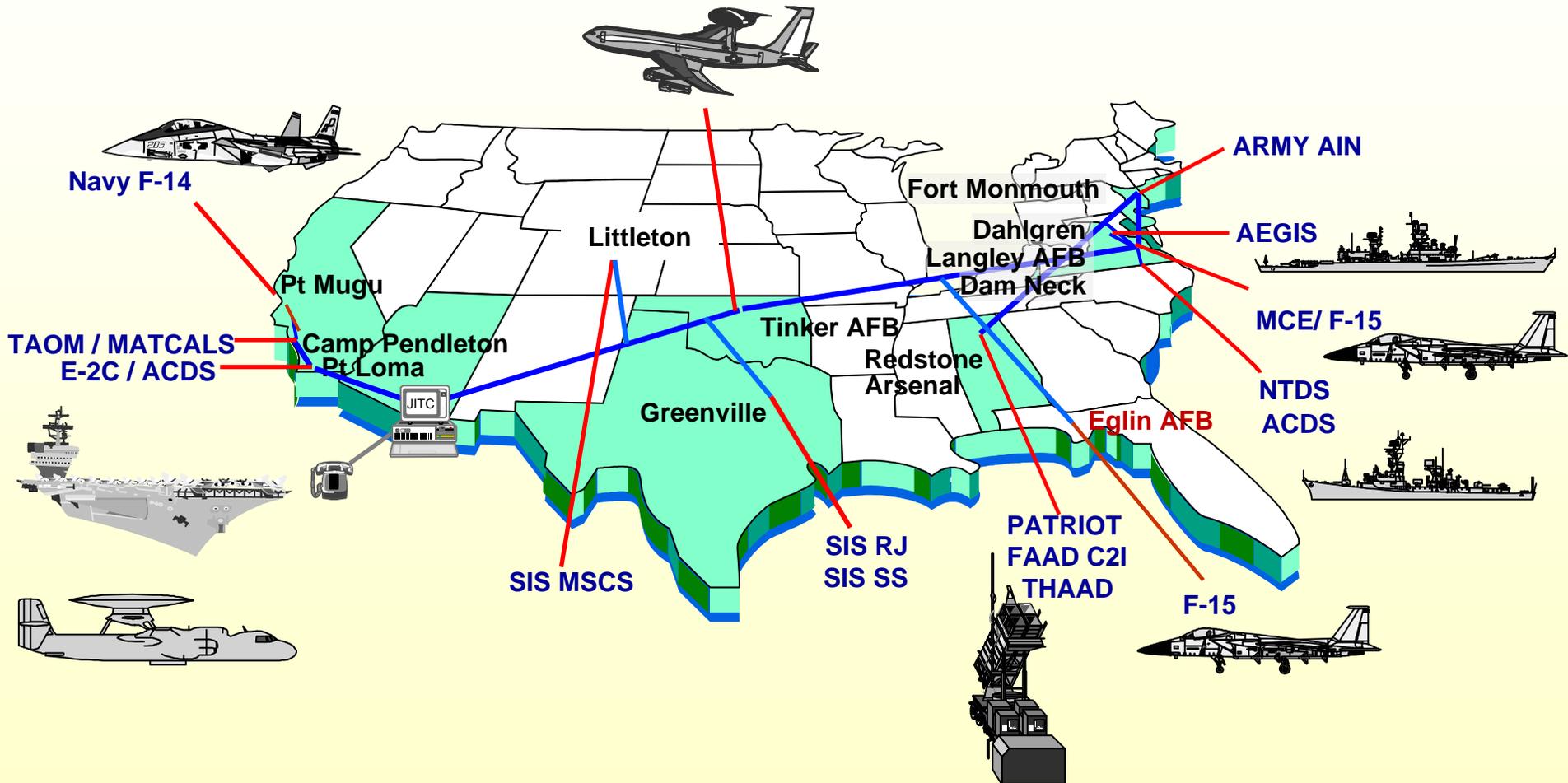


JTDL Lab

- **Work closely with Service and Agencies Participating Test Unit Coordinators (PTUCs), USPACOM, NATO**
- **Comprises two subsystems devoted to certification testing of tactical data link interfaces.**
 - **Joint Interoperability Modular Evaluation System (JIMES)**
 - **Joint Computer Aided Analysis Tool (JCAAT)**
- **Remote Test Facilities (RTF)**
- **Central Test Facilities (CTF)**



Tactical Data Link Distributed Network





UHF DAMA Lab



Mission:

To help ensure joint interoperability by verifying these terminals all meet the same requirements of three specific Military Standards

GOAL: Joint Interoperability



UHF DAMA Lab

- **CJCSI 6251.01A: MIL-STD Conformance**

- MIL-STD-188-181 (rev-, rev A, rev B)
- MIL-STD-188-182 (rev-, rev A)
- MIL-STD-188-183 (rev-, rev A)

Note: A single terminal version must be certified to all three MIL-STDs. Future mandate should also address interoperability

- **Interoperability Certification**

- Based on end-to-end testing in realistic environment
- Specific ORD & TEMP requirements define interoperability test
- Interoperability demonstrated during JMINI IOC Test, Jun 00



MIL-STD-188-181

5kHz & 25kHz Dedicated

- **BER Performance, Carrier Degradation**
- **Carrier Dropout**
- **Alternate Channel Emissions and Spectral Containment**
- **Adjacent Channel Emissions and Spectral Containment**
- **Adjacent Channel Interference Susceptibility**
- **Waveform Structure**
- **Unshaped BPSK**
- **Differential Encoding, FSK Modulation and Phase Noise**
- **Transmit and Receive Frequency Tuning Range and Accuracy**
- **Effective Radiated Power (EIRP) and EIRP Accuracy**



MIL-STD-188-182

5kHz DAMA

- **Login, Report Status and Logout**
- **Address Management**
- **Message Service Options**
- **Burst Type Determination**
- **FOW Dropout**
- **Contention ROW Message**
- **Network Entry/Rollover**
- **Terminal/System Restrictions**
- **Terminal Network Transition Protocol**
- **Service Preemption**
- **Retransmission Flag**
- **Future FOW Reception**
- **Contention Ranging Back-Off Algorithm**
- **Dedicated Channels**
- **Decoder Performance**
- **FOW Acquisition**
- **C/No Estimation**
- **Uplink Frequency Accuracy**
- **Adjacent Channel Emissions**
- **Multiple Channels**
- **Ranging**
- **COMSEC Interoperability Demonstration**
- **Multiple Hop Service Options**



MIL-STD-188-183

25kHz DAMA

- Preamble Measurements
- Random, Dedicated Ranging
- Slot Timing
- Range Uncertainty
- 25-kHz Ch Throughput Delay
- 5-kHz Ch Throughput Delay
- Adjacent Channel Emissions
- Uplink, Downlink Freq Accuracy
- Terminal Switching Time
- User COMSEC
- User Data COMSEC
- Bit Error Rate and Burst Acquisition Tests
- Master Frame
- Information Request/Information Report
- Link Report
- RCCOW Transmit Decision and Zeroize Command
- Encrypted Orderwire Operation
- Data Transfer
- Master Frame
- Slot Connect/Disconnect
- Link Test
- Special Format Change Order
- Call, Out of Service, and Paging
- TDMA Channel Reassignment
- DASA Channel Assignment
- Status and Guard List Reports
- Information Request and Report
- RCCOW Transmit Decision and Zeroize Command
- SAC Interoperability
- Data Transfer



WARFIGHTER / CUSTOMER BENEFITS

- **Verify radios are standards compliant**
- **Provide inexpensive “one-stop-shop” testing**
- **Discover UHF SATCOM terminal problems**
- **Improve the MIL-STDs**
- **Identify transmit power limits to reduce self-jamming**
- **Maintain web-based DAMA compliance registry**



SUCCESS STORIES

- Issued more than 300 conformance Cert's
- Anti-jam power limits for all tested terminals
- Resolved MIL-STD requirement ambiguities
- 25 kHz slave channel “proof of concept”



Joint Operational C4I Assessment Team

Hill 90, Osan AFB
FOAL EAGLE





JOCAT

- **A third generation field data collection and analysis capability that supports exercises, testing, and real-world contingencies.**
 - **Deployed to numerous joint/combined exercises**
 - **Foal Eagle**
 - **ASCIET**
 - **Roving Sands**
 - **Millennium Challenge**
 - **Deployments augment JITC's laboratory-based certification test process**

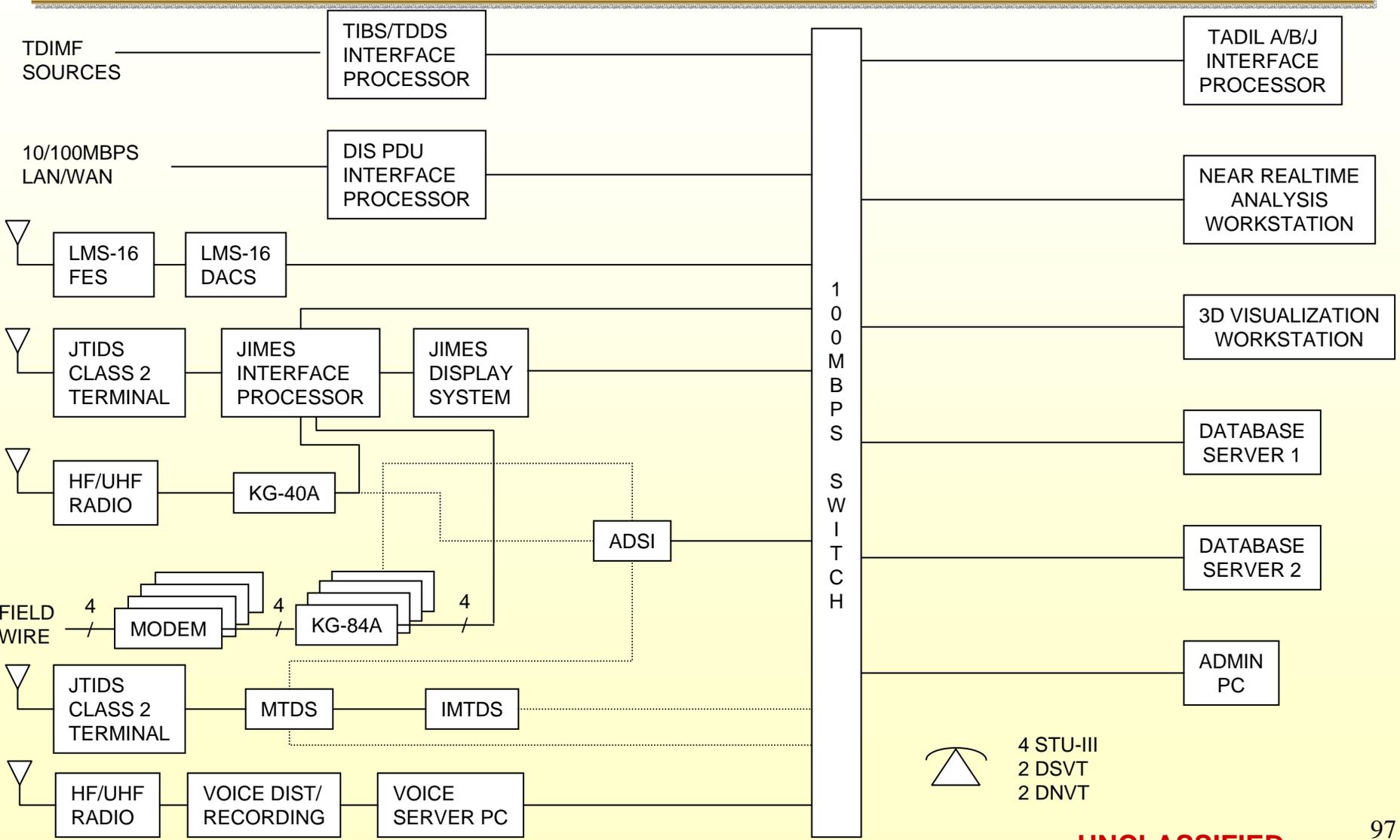


JOCAT

- **Collect, Record, and Time Stamp:**
 - Information exchange on Joint Data Network
 - Truth data from Distributed Interactive Simulation networks
 - Voice transmissions from tactical nets
- **Assess**
 - C4I interoperability effectiveness in terms of its affect on the accomplishment of operational objectives



Generic Architecture





JOCAT

- The **Team** and its **Tools** are used to:
 - Record
 - Monitor
 - Analyze **Events of Interest** (EOI) from:
 - Selected voice networks
 - JDN
 - TIBS
 - TRAP



JOCAT

- JOCAT **Team** of highly experience professionals:
 - Team Lead- AWACS Battle Manager
 - JOCAT Engineer
 - Software Engineers
 - Data Analysts
 - Additional Analysts, as required



JOCAT

- JOCAT Tools are a smart mix of:
 - COTS and GOTS
 - LMS-16
 - MTDS / IMTDS
 - ADSI
 - Digital voice recorder
 - In-house developed subsystems:
 - JIMES
 - Database and visualization tools



Real-time

- **JDN Interoperability Alerts**
 - Cues potential interop problems for further analysis
 - Reporting responsibility (R²) battles
 - ID / engagement anomalies
 - IFF / engagement anomalies
 - All engagements
 - ID conflicts



Real-time

- **Monitoring**

- Joint Data Network (TADILs A, B, J)
- Selected voice networks (HF, UHF, SATCOM)
- Exercise specific simulations/networks (DIS PDUs)



Near Real-time

- **During mission execution supports:**
 - Automated assessment of interoperability issues
 - Engagement analysis
 - Identification anomalies analysis
 - Track histories
 - Track management analysis (JICO support)
 - Other events of interest analysis



Post Event Analysis

- **Analyze Events of Interest**
 - Period of time each participant was in link
 - J-Message transmission conformance
 - Track number reuse / time slot allocation Isolate each EOI and compare to ground truth data
 - Determine if EOI tracks were reported completely, accurately, and quickly enough to be engaged
 - If not, determine nature of anomaly (tech or TTP)
 - Pursue technical anomalies to determine cause(s)
 - Recommend solutions to technical problems (PTR)



Post Event Analysis

- **Produce Final Report**
 - Identify all anomalies recorded
 - Determine root causes
 - Provide recommendations to improve future Link 16 performance



NITFS Compliance Test Facility

The logo for the NITFS Compliance Test Facility is rendered in large, 3D, metallic-style letters. The letters are white with a grey shadow on the bottom and right sides, giving them a three-dimensional appearance. The letters are arranged in a slightly descending line from left to right.

Mission:

**Serve as the NGA
Executive Agent for NITF
Compliance Testing.
Support Intelligence
Community and Coalition
Imagery Communities.
Strive for IOP of NITFS
Implementations.**



NITFS CTF

- **Capabilities:**

- **NITFS Compliance Testing**
- **Validation Testing of Standards and Sample Implementations**
- **Develop Software Test Tools**
- **Conduct NITFS Training (Basic to Advanced)**
- **Quick Analysis of NITF Products**
- **Rapid Prototyping of NITFS Test Files**



NITFS CTF

- **Major Test Equipment**
 - 10 Windows based PCs
 - 5 Sun/Solaris based Workstations
 - UNCLAS and Classified (Low & High) Ethernet networks
 - Latest NITFS Commercial Software Applications



NITFS CTF

- **Additional information:**
 - **Significant portion of funding is reimbursable**
 - **We work closely with or are able to assist**
 - **NITFS Software Developers**
 - **C/S/A supporting Imagery Dissemination**
 - **NATO Working Groups**
 - **ISO Committees**
 - **13 Years of experience in supporting the Imagery testing needs of DOD.**
 - **One of the first programs established to reduce interoperability problems found during Grenada Operation**



JBMC2 Roadmap Clusters

BACKUP



Six Program Interoperability Test Groups

1. **Single Integrated Ground Picture**
2. **Battlespace Awareness**
3. **“Flagship” BMC2**
4. **Single Integrated Air Picture**
5. **Operational C2**
6. **GIG-BE / IPv6**

Each Group has several Program “Clusters”



SIGP-Related Clusters

- **Cluster 1**
 - Army JBMC2 Systems
 - USMC JBMC2 Systems

- **Cluster 3**
 - Army Systems Upgrades / FCS

- **Cluster 4**
 - Army Systems Upgrades / USMC / FCS
 - Direct follow-on from Clusters 1 and 3



SIGP-Related Clusters

- **Cluster 1**

- **Army JBMC2 Systems (Software block X upgrades)**
- **USMC JBMC2 Systems**
- **Ensure current systems being upgrades as part of Army software blocking process are interoperable with current USMC systems**
- **Also, ensure responsive exchange of USA / USMC Joint Blue Force Situational Awareness information**



SIGP-Related Clusters

- **Cluster 3**

- **Army Systems Upgrades / FCS**

- **Ensure interoperability between FCS and current Army systems**
 - **Also, ensure these JBMC2 systems can responsively exchange JBFSA as well as targeting info to support future Army fire support and precision engagement mission threads**



SIGP-Related Clusters

- **Cluster 4**

- **Army Systems Upgrades / USMC / FCS**
- **Direct follow-on from Clusters 1 and 3**

- **Ensure all current and future Army ground systems are interoperable with each other and enable responsive sharing of:**

- **JBFS**
- **Joint ground force PE**
- **Integrated logistics information**

- **Last Cluster in SIGP-Related group**

- **No testing until FCS reaches maturity**



Battlespace Awareness Clusters

- **Cluster 2**
 - Service DCGS Variants

- **Cluster 6**
 - DCGS Variants / MC2A / ACS



Battlespace Awareness Clusters

- **Cluster 2**

- **Service DCGS Variants**

- **Ensure the service's main battlespace awareness programs are interoperable with each other to allow for genuinely joint and dynamic ISR operations and analysis.**
 - **Also, evaluate progress of incorporating DCGS common software services**



Battlespace Awareness Clusters

- **Cluster 6**

- **DCGS Variants / MC2A / ACS**

- **An expansion of Cluster 2. Seeks to ensure that all of the major “pathfinder” programs supporting the battlespace awareness capability are interoperable with each other allowing for truly joint and dynamic ISR operations.**
 - **Testing for this cluster will not begin until the MC2A and ACS programs show reasonable maturity**



“Flagship” Related Clusters

- **Cluster 5**
 - FCS / MC2A / GIG / NCES
- **Cluster 7**
 - FORCEnet / ACS / FCS / MC2A / GIG / NCES



“Flagship” Related Clusters

- **Cluster 5**

- **FCS / MC2A / GIG / NCES**

- **Ensure that the two future flagship programs of the Army and the Air force can effectively support Joint Close Air Support and Joint Fire Missions**



“Flagship” Related Clusters

- **Cluster 7**

- **FORCEnet / ACS / FCS / MC2A / GIG / NCES**

- **Ensure leading “pathfinder” programs are interoperable with each other to provide integrated JBMC2 capabilities, particularly TMD, CMD, TST, and dynamic BA and JFC2**
 - **FORCEnet segment is to ensure Navy’s integrated architecture is interoperable with ACS, FCS, and MC2A Joint mission threads**



SIAP-Related Clusters

- **Cluster 8**

- MC2A / FORCEnet / Army Software Upgrades

- **Comprises the primary “pathfinder” programs that are significant contributors or consumers of the air battlespace picture.**

- **For Army Software Upgrades, includes those programs that will be part of the SIAP portfolio i.e. FAADC2 and Patriot**



Operational C2 Related Clusters

- **Cluster 9**
 - DJC2 / JC2 / GCCS / NCES

- **Cluster 0**
 - DJC2 / JC2 / GCCS / FCS / MC2A / USMC
GIG / NCES



Operational C2 Related Clusters

- **Cluster 9**
 - DJC2 / JC2 / GCCS / NCES
 - **Ensure software programs supporting operational C2 are fully integrated or converged to include NCES underpinnings**



Operational C2 Related Clusters

- **Cluster 0**

- DJC2 / JC2 / GCCS / FCS / MC2A / USMC
GIG / NCES

- Ensure joint force and service operational C2 programs are interoperable with each other
 - Also, ensure “pathfinder” programs communicating directly with the operational C2 programs are interoperable with each other



GIG-BE / IPv6 Related Clusters

- **Cluster G**

- **FORCEnet / JC2 / DJC2 / GCCS / NCES
GIG-BE / IPv6**

- **Ensures “pathfinder” programs that will first use the GIG-BE / IPv6 expansions can do so properly**
 - **Consists of the operational C2 programs along with relevant components of FORCEnet**