DISA Testing Services for the Enterprise
Our Mission

DISA, a Combat Support Agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint Warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations.
Global Connectivity
Global Computing
Enterprise Services
Mission Assurance

In collaboration with COCOMs, Services, and Agencies
<table>
<thead>
<tr>
<th>Current</th>
<th>Capability</th>
<th>Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hundreds of Data Centers</td>
<td>Data Center Consolidation</td>
<td>Small Number of Shared Data Centers</td>
</tr>
<tr>
<td>Divergent Voice, Video, and Data Services</td>
<td>Unified Capabilities</td>
<td>Integrated Voice, Video, and Data Real-Time Collaboration</td>
</tr>
<tr>
<td>Service Oriented Security</td>
<td>Enterprise Security Architecture</td>
<td>COCOM Oriented Security</td>
</tr>
<tr>
<td>Blackberry and Cell Phones STIGs</td>
<td>Mobile Technology</td>
<td>Tablets, Application Stores Security Requirements Guides</td>
</tr>
</tbody>
</table>

Many IT Infrastructures | Joint Information Environment | Single DoD IT Environment
Paradigm shift to “Cloud Services”

- Services are developed and integrated to support missions
- Common services are consumed
- Enterprise services are centrally managed

- Consolidation of resources decrease human services
- More capability monitored with less resources due to reduced footprint
- Better S/A and faster C2 increase Cyber management

- Consistent & consolidated architecture
- Commonality and UC promotes reciprocity in security and interoperability
- Rapid scaling and On-boarding of new users
JITC Customer Profile from FY07

- DISA was 11% of the Business
- No other Business Systems or Enterprise Solutions under test.
- T&E in FY07 was program by program

JITC Customer Profile from FY10

- DISA is now 23.6% of the Business
- BTA, MHS, and NSA begin their business transformation into enterprise solutions, which totals 35.2%
- T&E in FY10 was still focused at a program level.
In FY12, just under half of all JITC business is in support of Enterprise solutions.

Chart to right depicts dollars not percentages.

- DISA is now 25.9% of the Business
- However, the trend shows Non-DISA organizations catching up.
- DLA (taking over from BTA) MHS, and NSA combined with DISA Enterprise Systems total 49.3%.
Anatomy T&E for Enterprise Services

Million’s of users exchanging Terabytes of data all the way to the edge.

It Takes More than One Organization to Create an Enterprise
Enterprise IT Service Management
Moving from Systems to Services

ITSM T&E Criteria

**Utility:** Fit for Purpose
- Improves performance and/or reduces constraints

**Warranty:** Fit for Use
- Reduce performance variation
  - Availability
  - Capacity
  - Continuity
  - Security

Enterprise Interoperability covered under **Utility** – Integrated services & Central management

**Security** directly tied to **Warranty**
Consistent products ensure a constant environment with reliable services.

Unified capability requirements support DISN (Network) and DISN Subscription Services (Voice, Video, Data, etc.).

Mobile Devices will use the same process, where security is key to approved for use.
Finally, the aim of DISA's architecture capabilities at the Command Level is to provide the Cyberspace Commander with situational awareness, critical information, alerts and warning, along with threat information to support C2 decisions based on full awareness and understanding. To defend against what we don’t know or expect.

DISA layers defenses at the Computing Infrastructure Level (local enclave environment) to protect critical programs, systems, enterprise services, servers (data) and host processing.

Applications, software and hardware are still required to comply with STIGs and IAVAs to protect against what we know.

At the program level, penetration testing is conducted. Security teams also conduct interviews and make observations at hosting locations. To protect against what we expect.

At the next layer, the Enterprise Infrastructure Level, DISA is embarking on the Enterprise Infrastructure Hardening initiative, a series of sensors, monitors, reaction and analysts systems to protect and defend critical enterprise infrastructure.

T&E processes and procedures, training and validation is what is missing and must be developed.

Achieving interoperability (systems, processes and people) of the cyberspace domain is critical to the defense of our networks, systems and information.

The DISA's Defense-in-Depth (DiD) architecture is designed to protect, detect, diagnose, react, and recover from hostile threats within the Global Information Grid (GIG).

At the Enterprise Infrastructure Level, DISA is embarking on the Enterprise Infrastructure Hardening initiative, a series of sensors, monitors, reaction and analysts systems to protect and defend critical enterprise infrastructure.

For Situational Awareness and Monitoring

Achieving interoperability (systems, processes and people) of the cyberspace domain is critical to the defense of our networks, systems and information.
Acquisition Planning Phase and is subject to change.

Classified and Unclassified Centralized Application Store with Decentralized Application Development by CC/S/A with MILDEP unique Enterprise Email (i.e. NMCI or AFNet)

SIM Cards procured by CC/S/A and registered on Management Servers

Centralized Government Management Servers
CC/S/A promotes Policies to Centralized Management Servers

Enables the mobile user access to secure commercial carrier transport and government enterprise services
DoD Enterprise Cloud Service Broker

DoD Consumers

T&E will likely focus on
V&V of services to broker, and performance and user experience post deployment.

Understand, collect, and aggregate DoD consumer requirements
Define services to be offered to DoD
Manage service provider relationships
Monitor performance
Match actual and anticipated user demand to current and future services
Integrate DoD Identity and Access Management
New Approach to T&E Services

Testing as a Service (Agile for the Enterprise)

- Interfaces, environments, services
- Automated script generation – agnostic
- SMEs to support performance, interoperability, security, etc events
- Single Security Architecture
- Platform as a Service
- Infrastructure as a Service
- Common services (Comms, capacity, etc)
- Government Acceptance Testing
- Hosting Environment Integration
- Central Management
- Consistent User Experience

SME support available as a consistent service to T&E customers
SUMMARY

• Department moving towards a converged Enterprise Service Environment
• DISA Architecting and Building the infrastructure and common services
• Services/Agencies shifting acquisition approach and require more than “functional” based automated T&E capability
• DISA/JITC working to enable environments, tools, services and SME’s into an enterprise “Testing as a Service” offering