Defense Information Systems Agency

Enabling The Joint Information Environment (JIE)

5 May 2014

Shaping the Enterprise for the Conflicts of Tomorrow

We must develop the JIE to secure our cyber infrastructure, cut costs, and be ready for tomorrow's technologies.

MAR 2012

DoD CIO

"Our primary goals are to make the Department ***more effective*** and ***more secure*** against cyber threats… …to ***reduce the cost*** associated with the Department's overall information technology infrastructure by simplifying, standardizing, centralizing, and automating infrastructure ***at the enterprise level***. We are calling the result of the effort the ***Joint Information Environment***, or ***JIE***." (Emphasis added)

Teri Takai, Former CIO, Department of Defense

JAN 2013

CJCS

"[With the JIE], we will have set the conditions for ***next generation capabilities***, fully leveraging the power and versatility of commercial information technology and evolving from a brittle, network-centric understanding of our information environment to ***a flexible data-centric environment*** enabling access to ***information at the point of need.***" (Emphasis added)

GEN Martin E. Dempsey, Chairman of the Joint Chiefs of Staff
(Joint Information Environment White Paper, Jan 2013)

THE JIE MISSION PARTNERS

THE JIE MISSION COMPONENTS

THE DRIVER

Capstone Concept for Joint Operations:
Joint Force 2020

10 September 2012

THE VISION

A single joint enterprise IT platform that can be leveraged for all DoD missions

THE STRATEGY

JOINT INFORMATION [illegible]

DEFENSE INFORMATION SYSTEMS AGENCY

STRATEGIC PLAN

[illegible]

DISA

DISA IS THE JIE TECHNICAL AND IMPLEMENTATION LEAD

DISA's JIE Technical Synchronization Office

Technical & Implementation Lead - Develop, integrate and synchronize JIE technical plans, programs, and capabilities and Execute JIE tasks

Key Functions:

- Develop DoD technical architectures
- Update EXCOM via Planning/Coord Cell
- Synchronize implementation activities with Transition Managers (CC/S/A)
- Recommend solutions for fiscal shortfalls
- Synchronize new capabilities & legacy IT sunsets
- Assess transition risk
- Synchronize with the IC Technology Enterprise

Key JIE Related Architecture Artifacts

Policy & Guidance

DoDI 8100.04

Establishes governing policy for Unified Capabilities products and services supported on DoD networks

9 DEC 2010

IdAM Data Dictionary

14 AUG 2013

DoDI 8330.aa

Establishes a capability-focused, architecture-based approach for interoperability analysis; Establishes the requirement for enterprise services to be certified for interoperability.

3QFY14

DoDI 8310.aa

Provides direction for identifying, developing, and prescribing IT standards

3QFY14

DoDI 8270.bb

Establishes the role of the DoD EA in providing context and rules for accomplishing the mission of the Department.

3QFY14

Enterprise Architecture

DoD IEA v2.0

Approved 10 Aug 2012; Foundation for the JIE EA

10 AUG 2012

JIE EA v0.4

In Formal Review; expected to be approved for JIE RA and SA development in 1QFY14

In progress

DoD IEA v3.0

Merges the architecture content and guidance of DoD IEA v2.0 and the JIE EA into a single, integrated, authoritative architecture for the Information Enterprise.

In progress

Reference Architectures

EANCS

24 AUG 2010

ADO RA

29 AUG 2012

UC RA

8 FEB 2013

SSA RA

MAY 2013

CDC RA

23 APR 2014

IdAM RA

23 APR 2014

EOC RA

In progress

EC RA

In progress

Solution Architectures

UC

30 AUG 2013

IdAM

30 NOV 2013

EOC

23 APR 2014

SSA-EPP

23 APR 2014

CDC

23 APR 2014

NNT-WAN

23 APR 2014

Key JIE Related Architecture Artifacts

Policy & Guidance

DoDI 8100.04

9 DEC 2010

Establishes governing policy for Unified Capabilities products and services supported on DoD networks.

IdAM Data Dictionary

14 AUG 2013

DoDI 8330.aa

3QFY14

Establishes a capability-focused, architecture-based approach for interoperability analysis; Establishes the requirement for enterprise services to be certified for interoperability.

DoDI 8310.aa

3QFY14

Provides direction for identifying, developing, and prescribing IT standards

DoDI 8270.bb

3QFY14

Establishes the role of the DoD EA in providing context and rules for accomplishing the mission of the Department.

Enterprise Architecture

DoD IEA v2.0

10 AUG 2012

Approved 10 Aug 2012; Foundation for the JIE EA

JIE EA v0.4

In progress

In Formal Review; expected to be approved for JIE RA and SA development in 1QFY14

DoD IEA v3.0

In progress

Merges the architecture content and guidance of DoD IEA v2.0 and the JIE EA into a single, integrated, authoritative architecture for the Information Enterprise.

Reference Architectures

EANCS

24 AUG 2010

ADO RA

29 AUG 2012

UC RA

8 FEB 2013

SSA RA

MAY 2013

CDC RA

23 APR 2014

IdAM RA

23 APR 2014

EOC RA

In progress

EC RA

In progress

Solution Architectures

UC

30 AUG 2013

IdAM

30 NOV 2013

EOC

23 APR 2014

SSA-EPP

23 APR 2014

CDC

23 APR 2014

NNT-WAN

23 APR 2014

"We need pioneers and visionaries and folks who are moving out to get us to where we need to go. We are not necessarily at a tipping point, but it is an informational point."

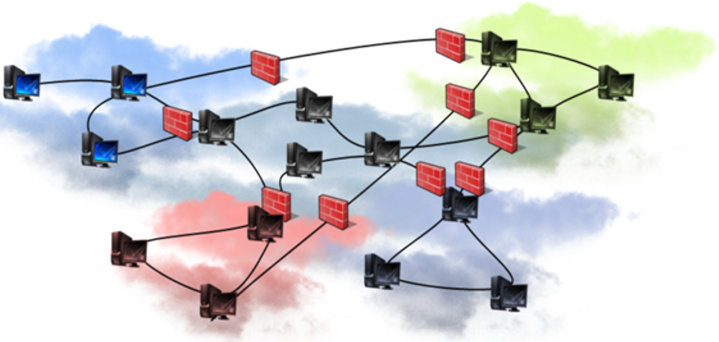
"...the expectations on this agency are huge, they are tremendous and people are expecting us to build this out"

-Lt Gen Ronnie D. Hawkins, Jr.,
Director, DISA

The DISA JIE Target State

Our target objective state is a Joint Information Environment that optimizes the use of the DoD's IT assets by converging communications, computing, and enterprise services into a single joint platform that can be leveraged for all Department missions. These efforts reduce total cost of ownership, reduce the attack surface of our networks, and enable DISA's mission partners to more efficiently access the information resources of the enterprise to perform their missions from any authorized IT device from anywhere in the world.

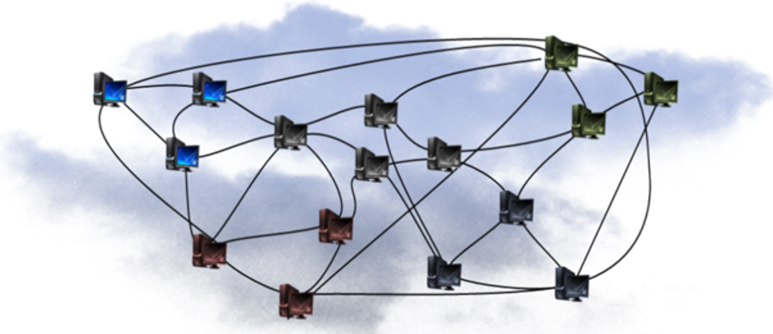
Imagine a road trip in a nation where each state only trusts vehicles and drivers from within its own borders. A trip from Nebraska to the West Coast requires border stops in Wyoming, Idaho, and Oregon, and a new driver's license must be obtained for each state. Now imagine some states have chosen to drive on the right side of the road and others on the left, while some only allow certain brands of vehicles on their roads. Imagine the headaches and difficulty encountered on a road trip from coast to coast.



This imagined road trip is what many warfighters face when attempting to access systems and information across the DoD. Delays in access to data due to differing systems, policies, and lack of trust between networks, affect the warfighter's ability to execute joint global military operations. At the same time, redundant infrastructure and services increase cost for the entire DoD. This can be solved by adopting a joint enterprise.

On our imagined road trip every state has its own dedicated border security, inspection stations, and monitoring equipment. A great deal of security infrastructure is focused on the highways between the states and not at the national borders. This slows down the flow of people and goods, leads to a heavier cost to implement security, and makes it difficult to share intelligence or coordinate operations across state lines. This imagined transportation system can be made more efficient by adopting a single national highway system, moving security infrastructure to the national borders, and implementing a common set of traffic laws.

Similarly, we can more efficiently communicate across the DoD with a joint enterprise. Communication and security infrastructure can be consolidated and utilized where it will be most effective, removing the barriers between mission partner networks. Most importantly, mobile warfighters will have access to the information and services they need when and where they need them.



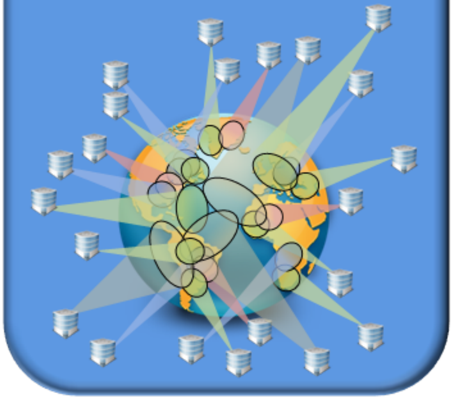
We will realize incredible efficiencies and cost savings by consolidating redundant capabilities at the enterprise level. For example, transitioning the Army to DoD enterprise e-mail alone is saving the service an estimated $100 million annually while providing greater e-mail capability than before.

The JIE is the DoD's enterprise solution. Improved interoperability within the JIE will be achieved through the integration and consolidation of our IT systems. This level of standardization and interoperability will allow more efficient collaboration between joint forces, the ability to provide joint cloud services, and reduce the cost of managing our IT infrastructure. More importantly, the JIE will give us the capability to deliver enterprise capabilities to the warfighter wherever, whenever.

Converging the C2 Infrastructure

The Pre-JIE DoD Enterprise

- No enterprise management
- Varying degrees of interoperability
- Lack of standardization
- Lack of cloud based services



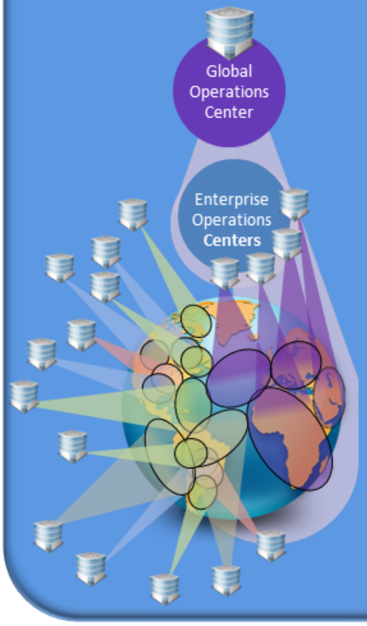
DoD Information Technology currently consists of thousands of IT systems, hundreds of globally unconnected data centers, and over seven million computer and IT devices. This infrastructure consists of:

- Service-centric non-standard operations centers
- Non-standard TTPs, architectures & applications
- No standard ops architectures

The JIE will begin to be realized with the convergence of the DoD IT infrastructure. The Interim JIE will see the establishment of:

- Standardized TTPs
- A Global Enterprise Operations Center (GEOC)
- Mixture of Regional Enterprise Operations Centers (EOC) and service led operations centers
- Initial JIE COP capability

JIE Interim

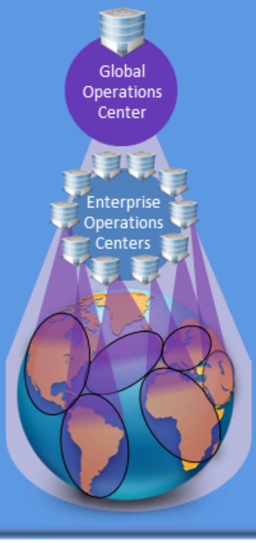


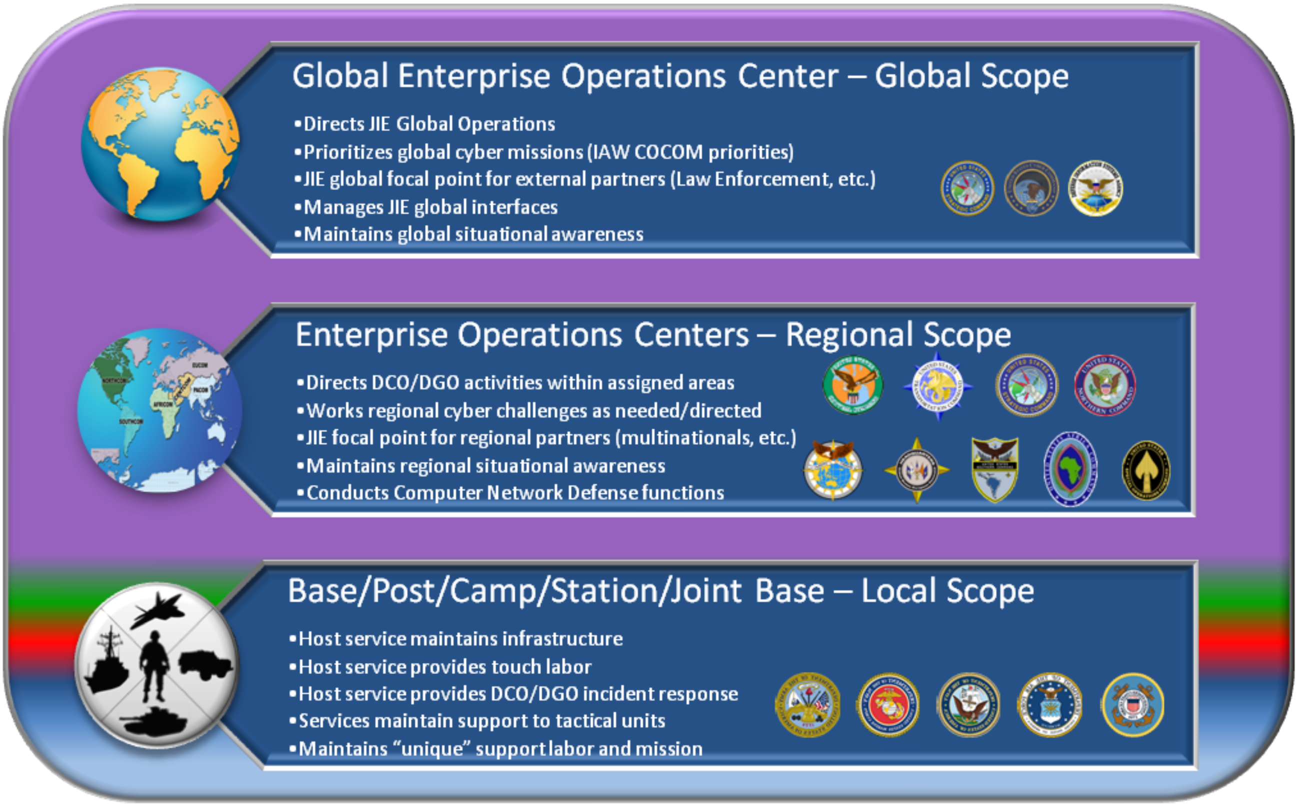
A major milestone in this transition was achieved in August 2013 with the stand up of the first regional EOC in Europe.

The JIE will ultimately provide the standardized framework for introducing new capabilities in an agile manner. This JIE end state will include:

- A Fully Operational GEOC
- Fully meshed EOCs providing seamless control and failover

JIE End State





Global Enterprise Operations Center – Global Scope

- Directs JIE Global Operations
- Prioritizes global cyber missions (IAW COCOM priorities)
- JIE global focal point for external partners (Law Enforcement, etc.)
- Manages JIE global interfaces
- Maintains global situational awareness

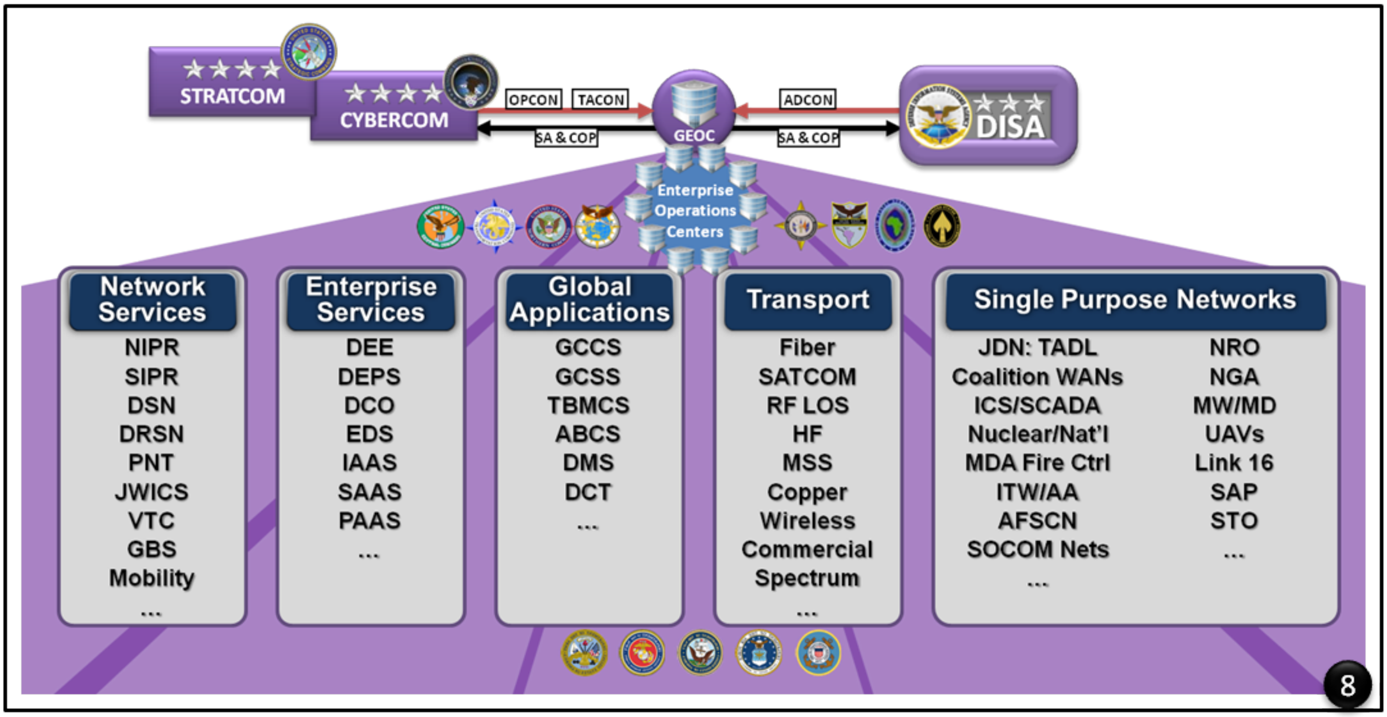
Enterprise Operations Centers – Regional Scope

- Directs DCO/DGO activities within assigned areas
- Works regional cyber challenges as needed/directed
- JIE focal point for regional partners (multinationals, etc.)
- Maintains regional situational awareness
- Conducts Computer Network Defense functions

Base/Post/Camp/Station/Joint Base – Local Scope

- Host service maintains infrastructure
- Host service provides touch labor
- Host service provides DCO/DGO incident response
- Services maintain support to tactical units
- Maintains “unique” support labor and mission

Management of the JIE will be a true joint endeavor. The GEOC will have complete visibility of the enterprise and will conduct global cyber operations in support of COCOMs. The regionally focused EOCs will have complete visibility into their portion of the enterprise, while conducting regional cyber missions supporting COCOM priorities, or supporting global missions directed by the GEOC. The services will continue to maintain their local infrastructure as well as the capabilities to support tactical units and service unique missions.



Network Services
NIPR
SIPR
DSN
DRSN
PNT
JWICS
VTC
GBS
Mobility
...

Enterprise Services
DEE
DEPS
DCO
EDS
IAAS
SAAS
PAAS
...

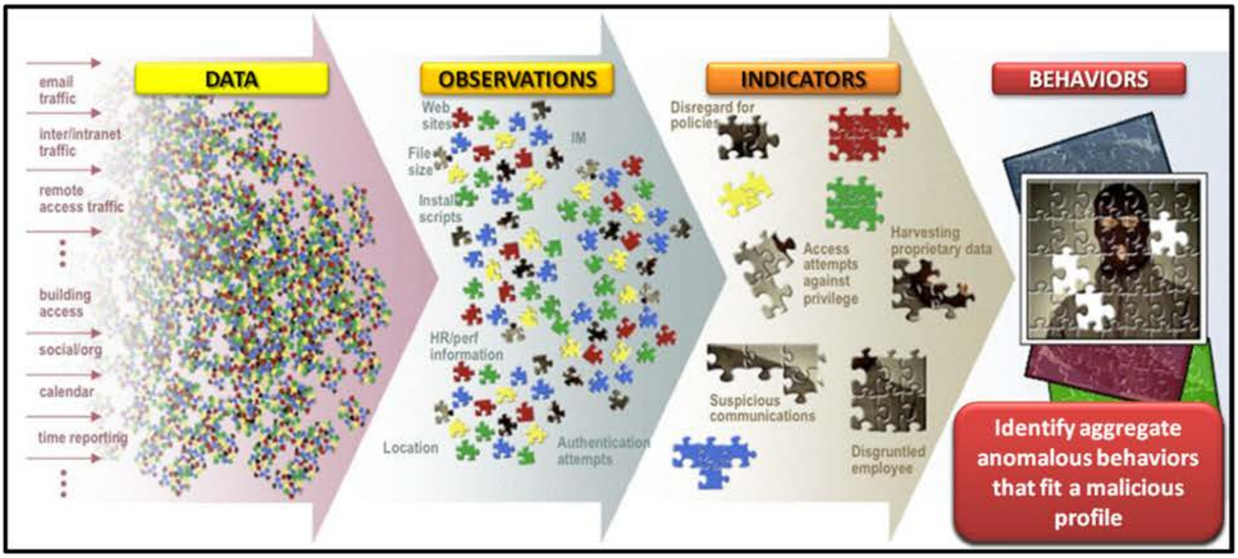
Global Applications
GCCS
GCSS
TBMCS
ABCS
DMS
DCT
...

Transport
Fiber
SATCOM
RF LOS
HF
MSS
Copper
Wireless
Commercial
Spectrum
...

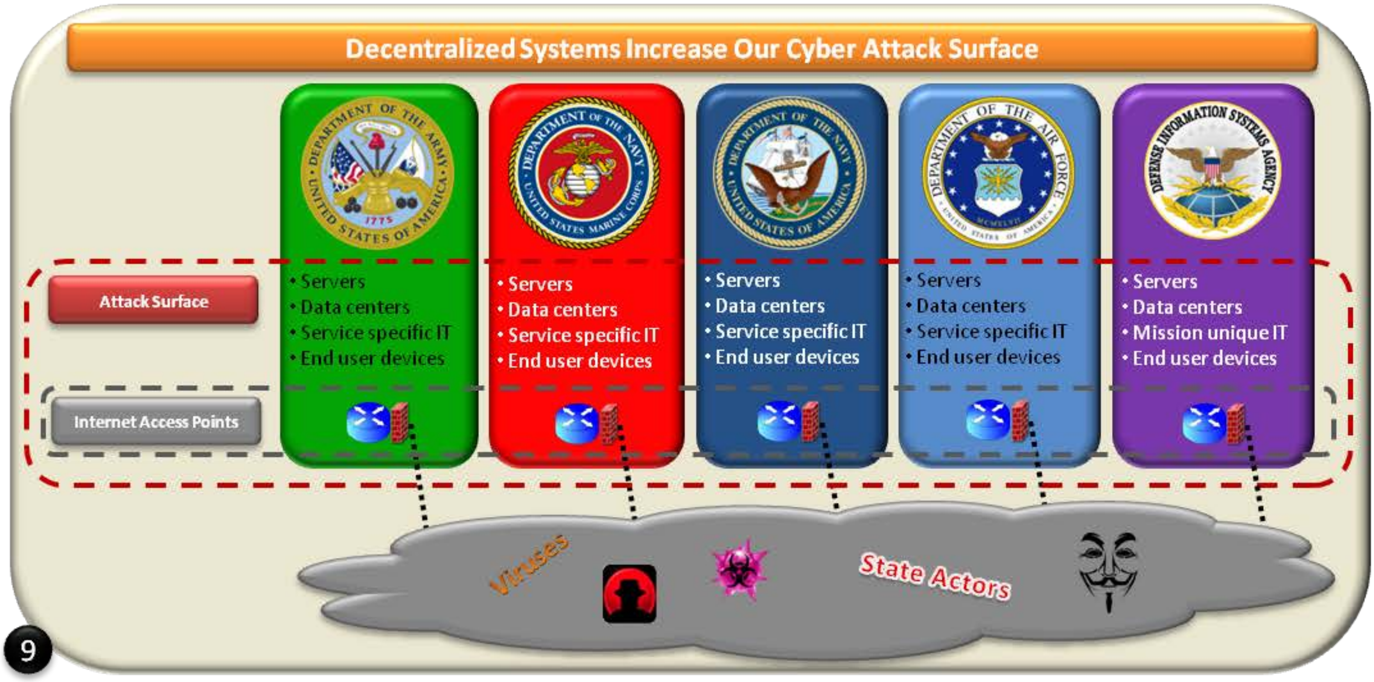
Single Purpose Networks
JDN: TADL
Coalition WANs
ICS/SCADA
Nuclear/Nat'l
MDA Fire Ctrl
ITW/AA
AFSCN
SOCOM Nets
...
NRO
NGA
MW/MD
UAVs
Link 16
SAP
STO
...

Toward a Single Security Architecture

Developing the JIE will enable us to actively defend our cyber infrastructure by constructing a SSA that will allow us to analyze and understand what is going on inside and across the entire enterprise. The identification of anomalous behavior is critical to combating the insider threat. The SSA is key to allowing visibility and Command & Control across all DoD networks.



Infrastructure convergence will not only eliminate inefficiencies in the routing of information, but will also focus security processes and infrastructure to where they will be most effective. Today our security infrastructure is focused at network boundaries. Each organization has built its own defensive architecture that, while defendable, is less secure and more obtrusive to information sharing than a consistent Joint solution. Further, our cyber attack surface is widened by the myriad systems providing decentralized IT services all across the DoD. Every e-mail server, end user, or network device is a potential target for a cyber attack. It is not feasible to properly secure every device, every capability, and every mission given our current architecture and need to share/access information.



Single Security Architecture

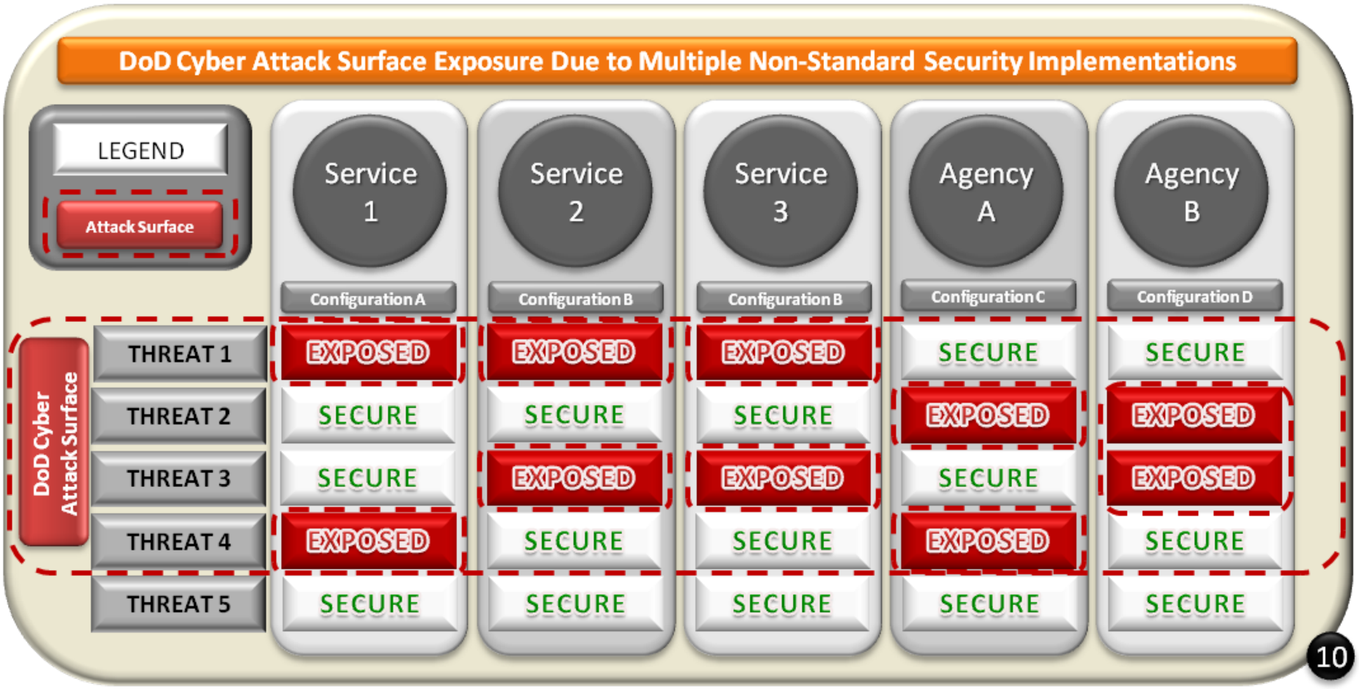
- Reducing our Cyber Attack Surface

Our ability to defend our current IT infrastructure is also complicated by decentralized configuration management and non-standard security implementations that widen our exposure to cyber threats. We successfully identify a policy or control to protect ourselves from a threat but must wait for that security control to be implemented throughout the entirety of the DoD. With our current infrastructure we must trust that the security control is eventually deployed to the rest of our networks in a timely manner, without human error, and without the ability to immediately verify that the control is in place.

> "Today we've got a lot of decentralized implementations of some pretty sophisticated and robust capabilities. But they're implemented in pockets, so we don't share information across all the pockets and don't have the ability to simultaneously change policies or controls across all those pockets instantly or at the same time."
>
> – Mark Orndorff, DISA
> Chief Mission Assurance Executive

The current system creates too many opportunities for failure and leads to unnecessary exposure of our cyber assets. Additionally, every misconfigured system that is vulnerable to a threat leaves the rest of the enterprise just as vulnerable and further expands our cyber attack surface.

The centralized JIE and Single Security Architecture will reduce our cyber attack surface by enabling centralized configuration management, along with standardized and simultaneously deployed security implementations.



DoD Cyber Attack Surface Exposure Due to Multiple Non-Standard Security Implementations

LEGEND
Attack Surface

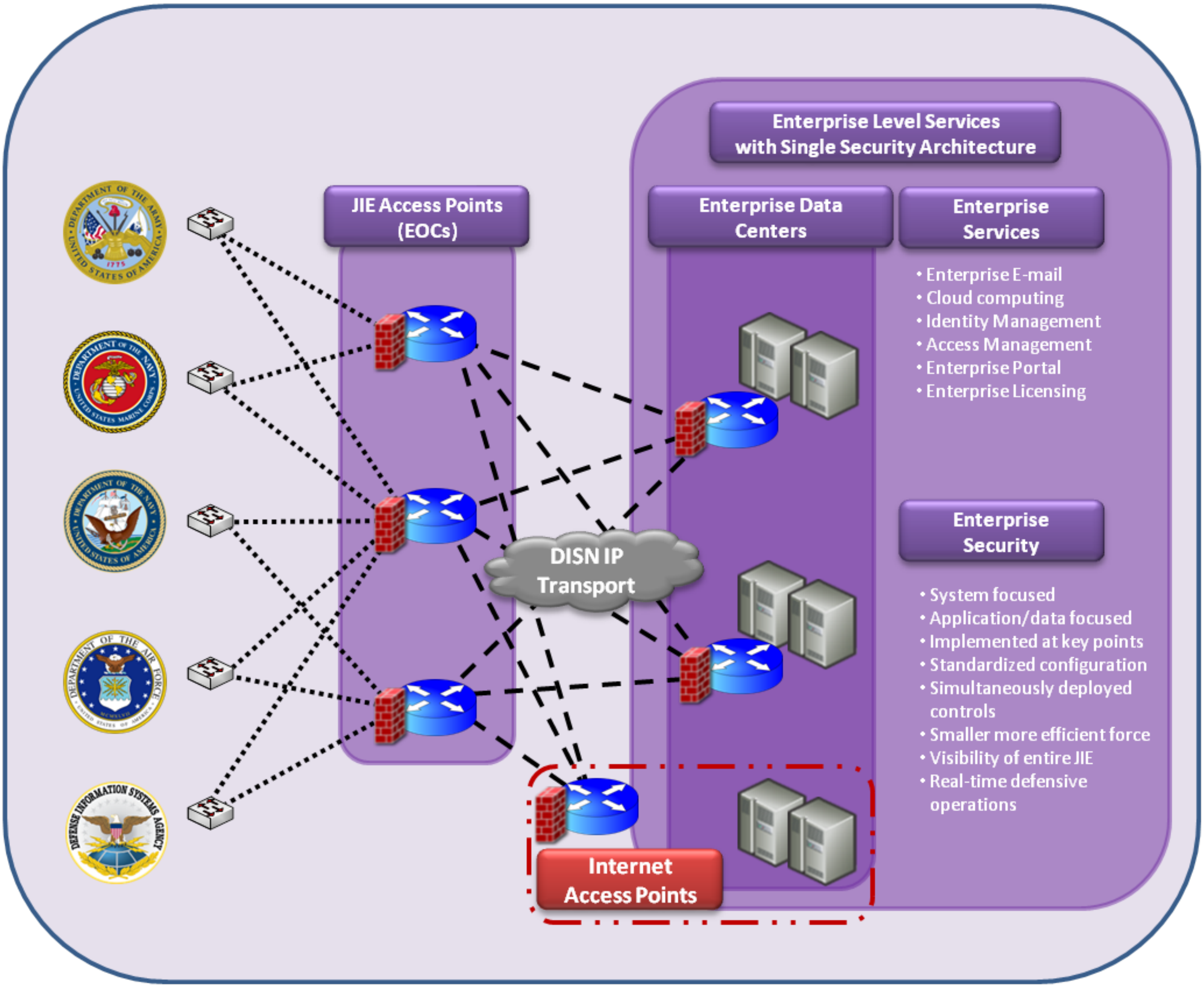
DoD Cyber Attack Surface

	Service 1	Service 2	Service 3	Agency A	Agency B
	Configuration A	Configuration B	Configuration B	Configuration C	Configuration D
THREAT 1	EXPOSED	EXPOSED	EXPOSED	SECURE	SECURE
THREAT 2	SECURE	SECURE	SECURE	EXPOSED	EXPOSED
THREAT 3	SECURE	EXPOSED	EXPOSED	SECURE	EXPOSED
THREAT 4	EXPOSED	SECURE	SECURE	EXPOSED	SECURE
THREAT 5	SECURE	SECURE	SECURE	SECURE	SECURE

Single Security Architecture

The JIE will allow us to more effectively secure the enterprise by consolidating services at enterprise data centers. Rather than trying to defend everything, security can then be focused on the systems and data needed to support specific missions and capabilities.

The SSA will reduce our exposed cyber attack surface and standardize our security practices to protect our networks and the information traversing them. The SSA will also increase the availability of Enterprise-wide services, applications and data sharing.



- Enterprise E-mail
- Cloud computing
- Identity Management
- Access Management
- Enterprise Portal
- Enterprise Licensing

- System focused
- Application/data focused
- Implemented at key points
- Standardized configuration
- Simultaneously deployed controls
- Smaller more efficient force
- Visibility of entire JIE
- Real-time defensive operations

"The No. 1 most important advantage [with the Single Security Architecture] is the ability to actively defend the DoD networks in a time frame that we need to execute cyber defensive operations. What I mean by that is the single security architecture will allow us to understand what's going on across the entire DoD network with global cyber situational awareness to a level that we can't do today."

- Mark Orndorff, DISA Chief Mission Assurance Executive

DISA Core Enterprise Services

The JIE will bring enterprise services that will enable true joint collaboration and reduce costs across the entire DoD. These solutions are in varying stages of implementation and endorsement as enterprise services. DISA will continue to provide and expand these offerings to meet the ever changing needs of the Warfighter.

> "We need to ***be prepared to collaborate*** all along the way… …cloud, virtualization, interoperability — it's there today. ***We can go with enterprises and save money***. Enterprise licenses between the Army, Air Force and DISA. You save tons of money there."
>
> *LTG Mark Bowman, J6/CIO,*
> *Joint Chiefs of Staff*

DEE

Defense Enterprise E-mail

DEPS

Defense Enterprise Portal Services

DCO

Defense Connect Online

UC

Unified Capabilities

Cloud Broker

Enterprise Cloud Broker

PAAS SAAS IAAS Computing Services

Cloud Computing Services

EDS

Enterprise Directory Service
Identity and Access Management

DEM

Defense Enterprise Mobility

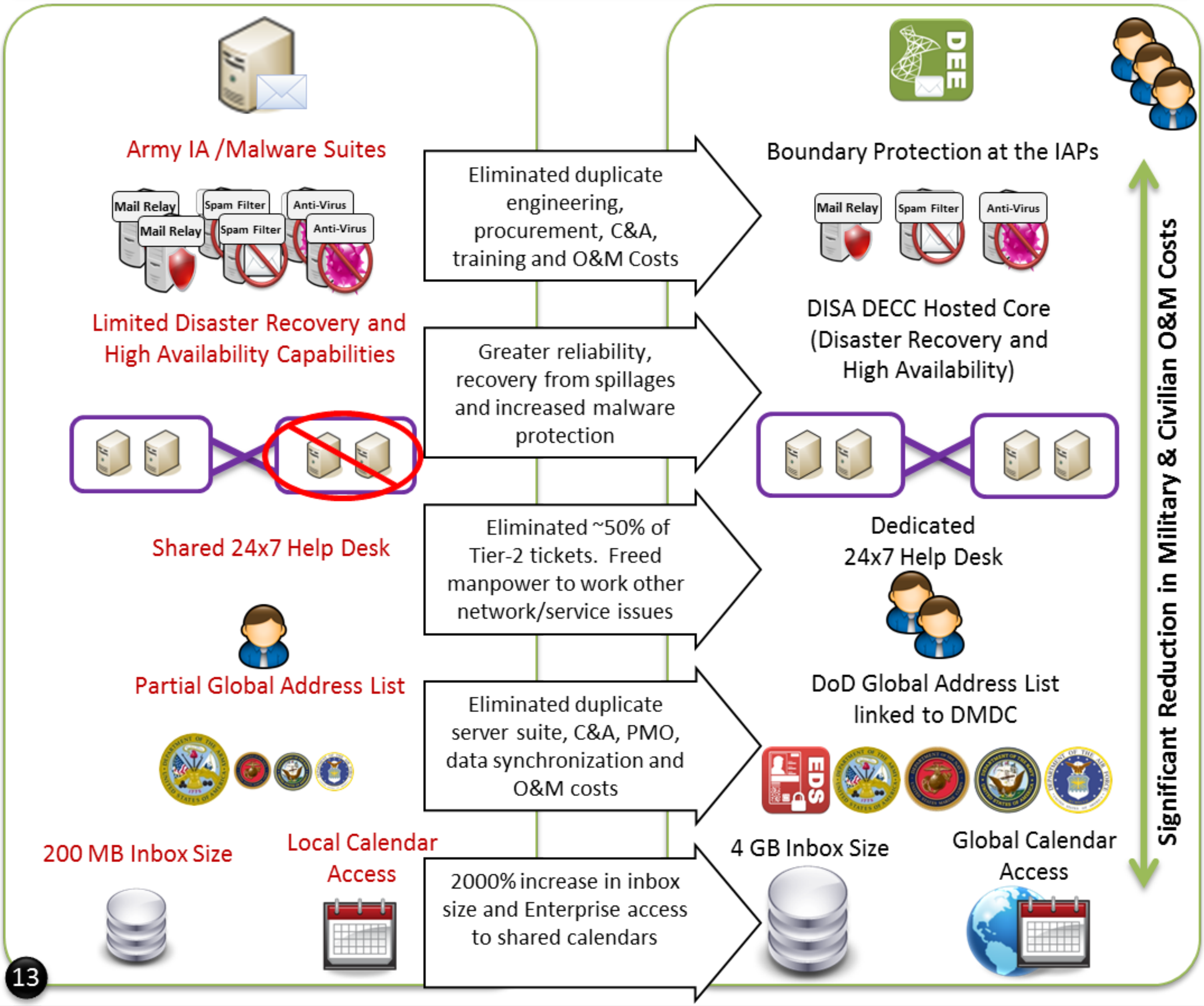
Defense Enterprise E-mail

On September 5, 2013, the DoD CIO mandated that all services transition to Defense Enterprise E-mail (DEE), recognizing the significant costs savings potential in this already fielded enterprise solution.

The Army's adoption of DEE resulted in a cost savings of $76 million for FY12 and projected cost savings of $100 million annually

Defense Enterprise E-mail offers greater capabilities at a cost below what individual organizations within the DoD can achieve on their own. DEE provides users a single e-mail address that follows them throughout their career, a four gigabyte e-mail storage capacity, and the ability to access e-mail through mobile devices. Joint collaboration is enhanced through a DoD Global Address List and enterprise wide calendar sharing.

Benefits of transitioning 1.5M Army users to DEE



Army IA /Malware Suites

Eliminated duplicate engineering, procurement, C&A, training and O&M Costs

Boundary Protection at the IAPs

Limited Disaster Recovery and High Availability Capabilities

Greater reliability, recovery from spillages and increased malware protection

DISA DECC Hosted Core (Disaster Recovery and High Availability)

Shared 24x7 Help Desk

Eliminated ~50% of Tier-2 tickets. Freed manpower to work other network/service issues

Dedicated 24x7 Help Desk

Partial Global Address List

Eliminated duplicate server suite, C&A, PMO, data synchronization and O&M costs

DoD Global Address List linked to DMDC

200 MB Inbox Size

Local Calendar Access

2000% increase in inbox size and Enterprise access to shared calendars

4 GB Inbox Size

Global Calendar Access

Significant Reduction in Military & Civilian O&M Costs

Defense Enterprise Portal Service

The Department of Defense Enterprise Portal Service (DEPS) provides a scalable, cloud-based collaboration capability that enables mission partners to share information through independently managed community and mission-focused sites. Built upon industry leading commercial-off-the-shelf solutions, DEPS enables site customization and content management to leverage standard taxonomy and templates. Using a common platform, DEPS enhances enterprise-wide collaboration and increases operational efficiency by leveraging highly secure Defense Enterprise Computing Centers (DECCs), which consolidate administrative, hardware, and software resources .

DEPS currently serves DoD level agencies, but DISA has the capability to grow capacity to support the entire DoD. DEPS provides redundancy both locally and remotely for all components of the system, replicating data between paired sister sites to facilitate Continuity of Operations Plans (COOP). DISA integrates DEPS customer organizations into the operational structure and provides 24/7 support through a central service desk.

DEPS Capabilities

- CAC Authenticated Access
- Basic Workflows
- DoD Address List
- Intranet Sites
- Document Libraries
- SharePoint Designer Access
- Team Sites / Calendars
- Real-time Collaboration
- SharePoint Lists
- Wikis / Blogs

DEPS is Integrated with:

Enterprise Directory Service
Identity and Access Management

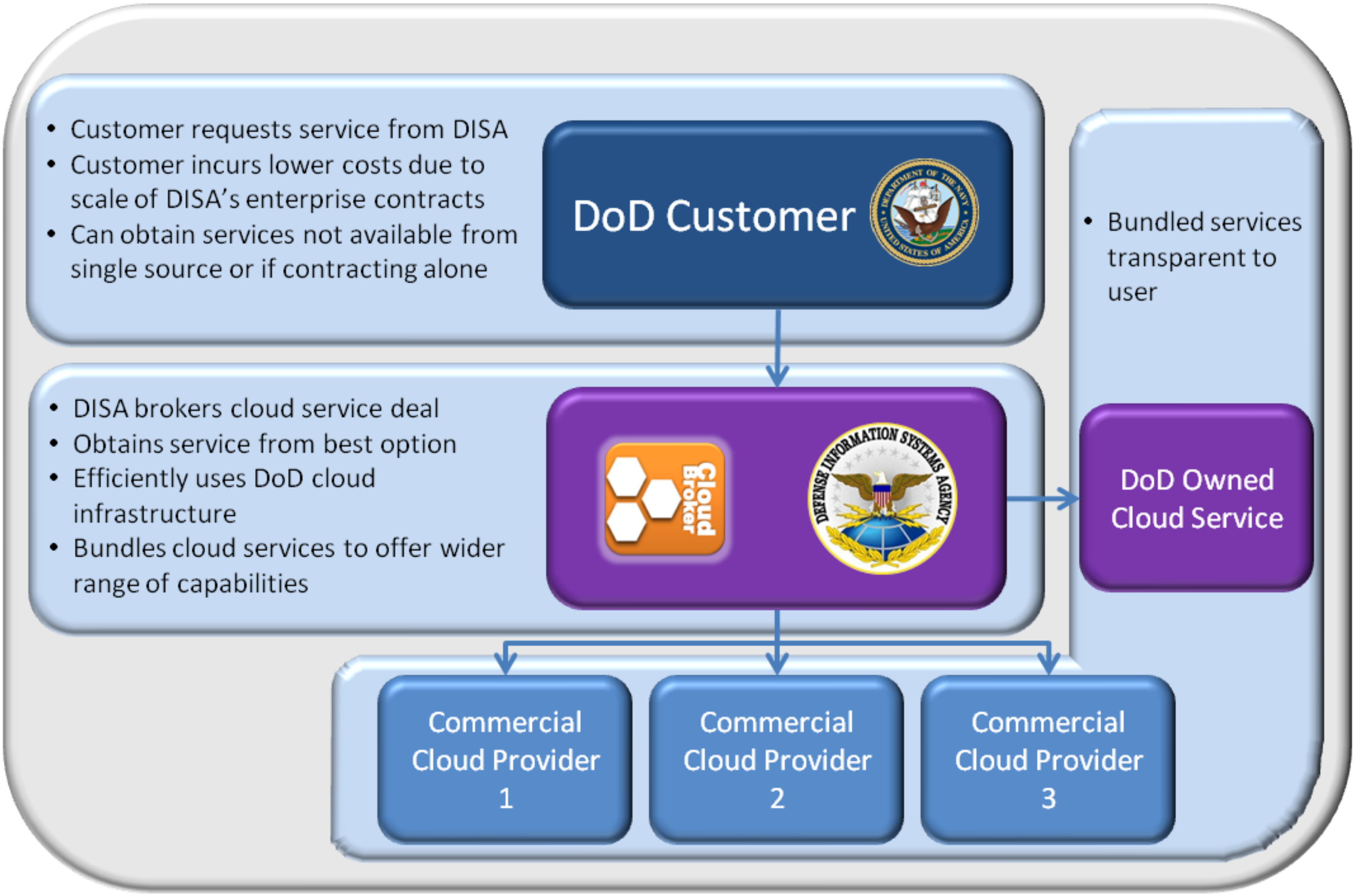
Defense Enterprise E-mail

Defense Enterprise Mobility

Unified Capabilities

Enterprise Cloud Broker

As the DoD enterprise cloud broker, DISA will speed up cloud service utilization and procurement through a consolidated departmental and commercial cloud delivery service. As the cloud broker, DISA is responsible for data integration and ensuring the security and movement of data between the cloud consumer and multiple cloud providers. This brokering service will allow organizations throughout the Department to realize cloud-based capabilities more efficiently and effectively due to the scale of enterprise contracts and consolidation of DoD cloud infrastructure.



- Customer requests service from DISA
- Customer incurs lower costs due to scale of DISA's enterprise contracts
- Can obtain services not available from single source or if contracting alone

- DISA brokers cloud service deal
- Obtains service from best option
- Efficiently uses DoD cloud infrastructure
- Bundles cloud services to offer wider range of capabilities

- Bundled services transparent to user

DoD Customer
Cloud Broker
DoD Owned Cloud Service
Commercial Cloud Provider 1
Commercial Cloud Provider 2
Commercial Cloud Provider 3

DoD Cloud Computing Goal

Implement cloud computing as the means to deliver the most innovative, efficient, and secure information and IT services in support of the Department's mission, anywhere, anytime, on any authorized device.

Data Center Consolidation

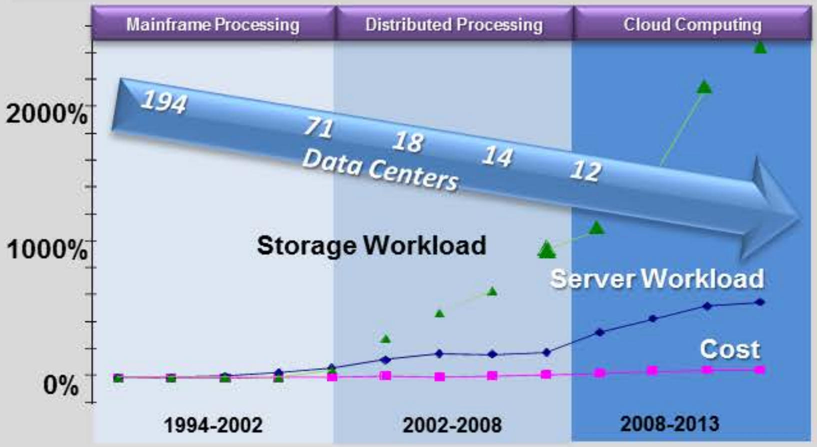
Cloud Computing Services

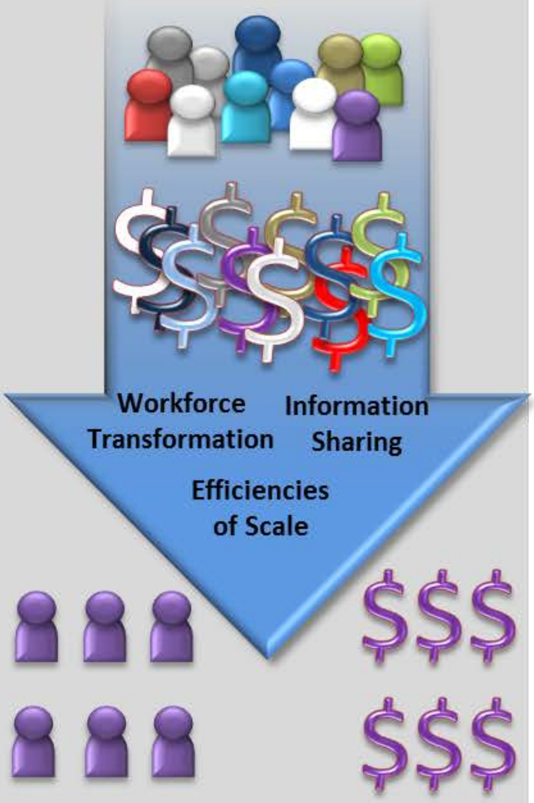
Enterprise Cloud Broker

Many of the JIE related cost savings are due to the consolidation of datacenters across the DoD. These consolidations have been taking place for nearly two decades but are now a major component of the evolution of the JIE. Since 2009, DISA sponsored data center consolidation efforts have led to:

FY09-FY12: Reduced Defense Enterprise Computing Center costs by $113.5 million annually

- All mainframe processing moved to two DECCs ($5 milion annually)
- GCCS-AF & AF Logistics systems consolidated ($14.9 million annually)
- Closed two DECCs ($7 million annually)
- Manhour reduction of over 10K Full Time Equivalent positions; $58 million FY09-12 tech refresh savings





Enterprise Directory Service Identity and Access Management (IdAM)

Enterprise Directory Services (EDS) is a suite of services that provide authoritative DoD enterprise identity and contact attributes for Combatant Commands, Services, and Agencies. EDS is composed of DoD Enterprise White Pages, Global Directory Service (GDS), and Identity Synchronization Service.

In the JIE, EDS will provide IdAM for person entities and non-person entities operating within the DoD Enterprise.

Current EDS Services

DoD Enterprise White Pages

A web based search utility where DoD personnel can retrieve authoritative identity and contact information for all DoD Common Access Card (CAC) holders.

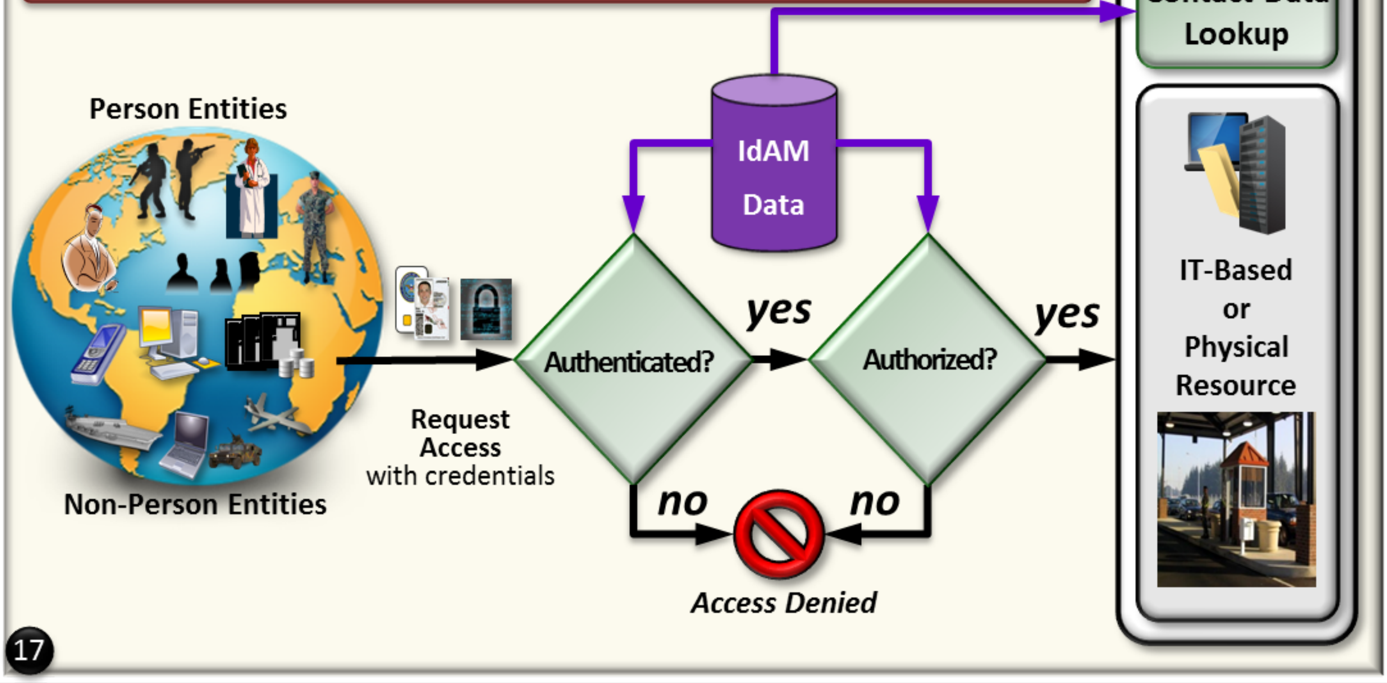
Global Directory Service

A distribution point for personnel Public Key certificates, Certificate Authority (CA) Certificate Revocation Lists (CRLs), and CA certificates

Identity Synchronization Service

A service utilized to populate Combatant Command, Service and Agency directories and Global Address Lists (GALs) with authoritative enterprise identity and contact attributes.

Enterprise Identity and Access Management

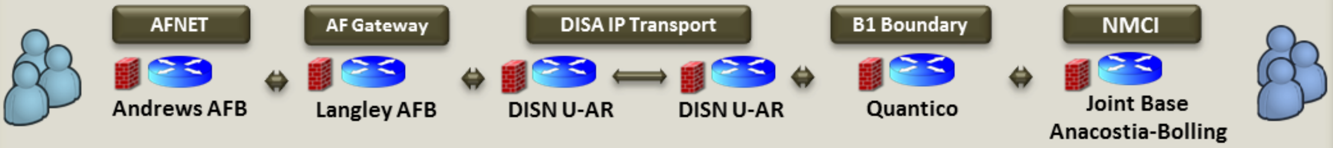


Unified Capabilities

Unified Capabilities (UC) includes a broad set of voice-, video- and data-sharing capabilities that promise to enable unprecedented joint collaboration among the military services, combatant commands and defense agencies. IP-based solutions will enable DoD users to better collaborate via instant messaging, chat, enterprise voice-over-IP (VOIP), global video services, IP video, Web conferencing and unified messaging, among other applications.

> "We know that it's five times more expensive to maintain a legacy telephony network versus an IP-based converged environment."
>
> \- Cindy Moran, Director, Network Services
> DISA

Existing Architecture Example



Troubleshooting requires coordination from:

- AF Base Sys Admin (Andrews AFB, MD)
- I-NOSC East (Langley AFB, VA)
- 26th Network Ops Sq (Gunter Annex, AL)
- DISA CONUS (Scott AFB, IL)
- DISA GIG Ops (Ft Meade, MD)
- PMW-130 (Naval Base San Diego, CA)
- NMCI NOC (Naval Station Norfolk, VA)
- MCCC / MAJCOM PMO

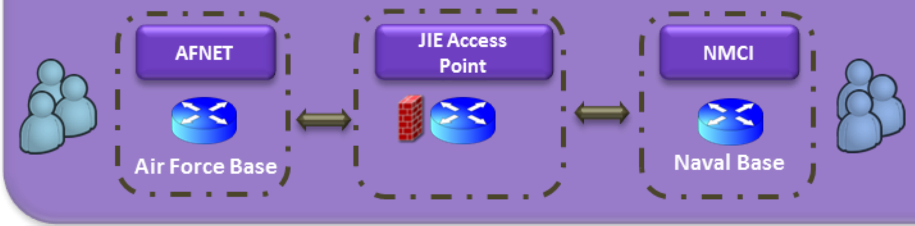
~4025 TDM B/P/C/S switches

TDM

Annual O&M = $500M

By offering all of these services over IP the Department avoids the duplication of costs for voice services, operations and maintenance, network operations, sustainment and information assurance at nearly 2,000 locations worldwide with a lower total cost of ownership.

Future Architecture Example



- Fewer Network Layers
- No Backhauling Data
- Fewer Deep Packet Inspections
- Standardized Equipment Suites
- Streamlined Troubleshooting

- Joint forces communicate more seamlessly
- Leaner infrastructure is cheaper and easier to manage and maintain
- Fewer systems exposed to potential cyber attack; reduced cyber attack surface

18 DoD Soft switches &
93 session controllers

IP

Annual O&M = $100M

Defense Enterprise Mobility

Mobility is transforming how the Department of Defense operates, connects, and supports its stakeholders — most significantly, using mobile solutions to provide mission-essential tools to our warfighters. Mobility is a key component of the goal to enable mission partners to perform their missions and connect to the Joint Information Environment, using any authorized device, anytime, anywhere in the world.

The focus is on "building the foundation" — designing governance processes and implementing an integrated Mobile Device Manager (MDM), Mobile Application Store (MAS), mobile Virtual Private Network (VPN), and other mobile capabilities.

DISA is working to streamline the deployment of mobile devices and services across the DoD through changes in both architecture and acquisition. To provide mobile services, DISA is contracting with commercial carriers capable of handling classified data. DISA is also reengineering its approach to how we evaluate devices and create Security Technical Implementation Guides (STIG) for their secure installation and deployment.

> "This is not simply about embracing the newest technology, it is about keeping the department's workforce relevant in an era when information accessibility and cybersecurity play a critical role in mission success."
>
> \- Ms. Teri Takai, Former CIO, Department of Defense

Previously, the STIG development process often took so long that a mobile or enterprise technology could be obsolete by the time it was approved for use on DoD networks. By partnering with industry, DISA can now have a device approved for use on the DoD enterprise at the same time it is brought to the commercial market.

Streamlined Device Approval Process

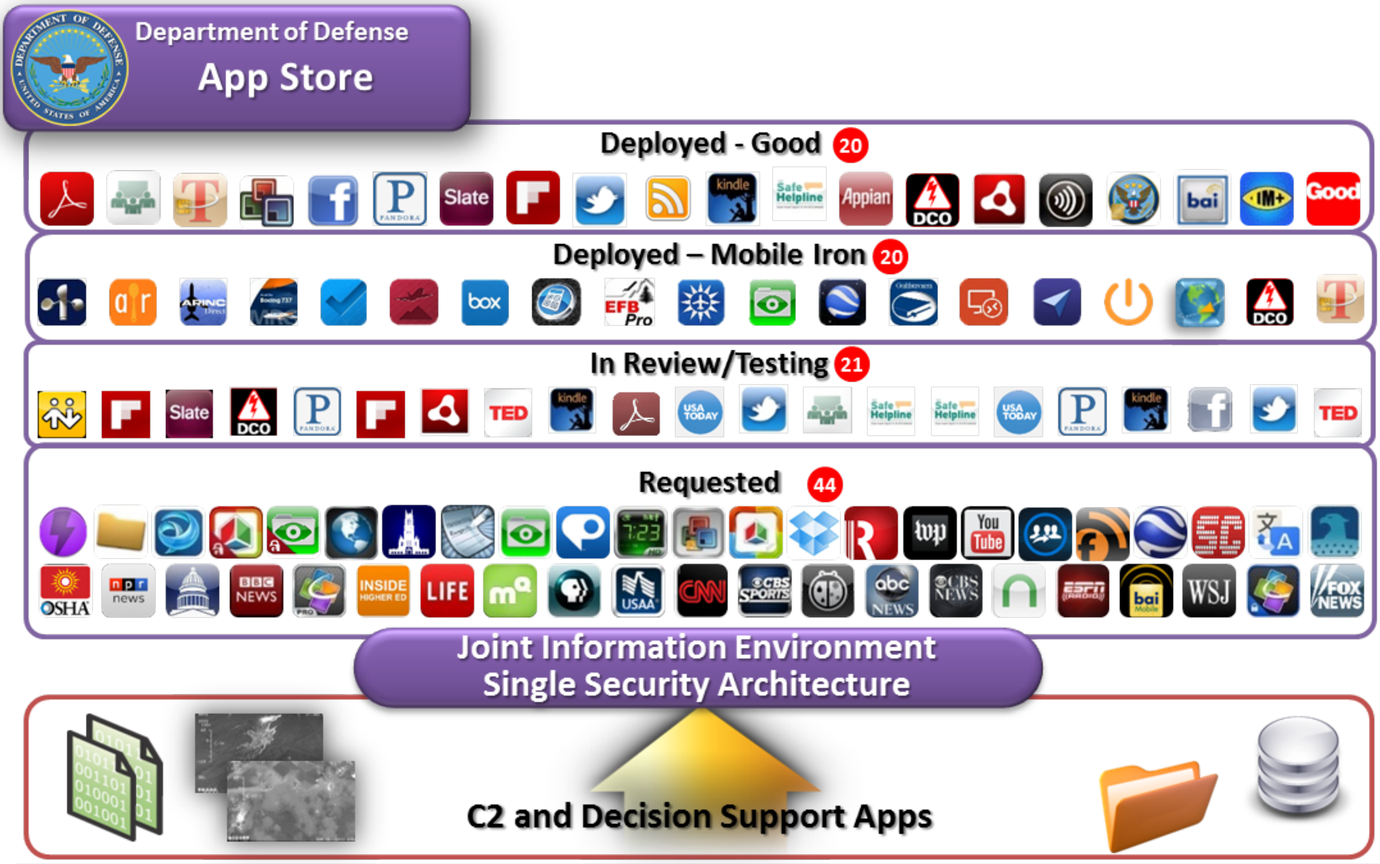
- DISA specifies IA requirements
- Industry develops device and writes STIG IAW IA guidance
- Device and STIG are delivered simultaneously
- DISA reviews device and STIG for compliance
- Device is approved for DoD use at same time as release to commercial market

The DoD App Store

Mobile devices will provide access to the DoD Information Networks (DoDIN), allowing warfighters to operate within the JIE when and where needed. The JIE will provide access to the information that the warfighter needs. But it is applications that will provide the toolkits to take advantage of that information.

The DoD CIO's goal is to develop an overall governance process, a centralized library, and a development framework in which mobile applications can be quickly developed, purchased, certified and distributed to users. DISA is once again challenged to meet this goal.

DISA will develop an unclassified enterprise Mobile Application Store (MAS) that will deliver, update and delete applications on mobile devices without the user having to return the device for service. The functionality will be similar to that found in commercial app stores, and will contain both commercially available apps and those created for exclusive use within the DoD. Eventually a similar system will be developed for classified devices.



Department of Defense App Store

Deployed - Good 20

Deployed – Mobile Iron 20

In Review/Testing 21

Requested 44

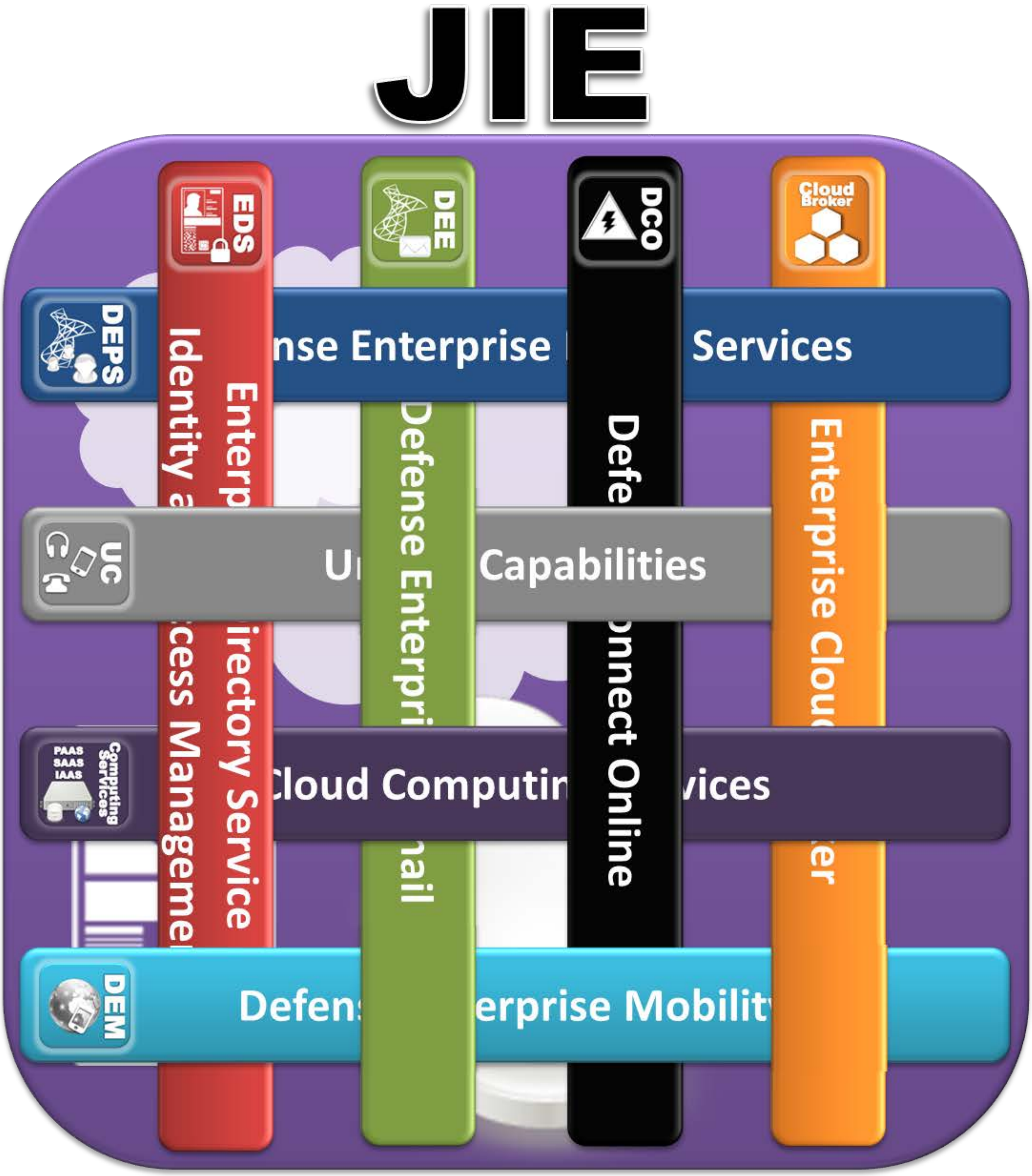
Joint Information Environment Single Security Architecture

C2 and Decision Support Apps

JIE SSA will Break Down the Barriers Allowing Mobile Access to C2 and Decision Support Information

Enabling the JIE

DISA's interwoven enterprise solution set will enable the JIE to deliver and protect the information-driven capabilities the warfighter deserves and needs to accomplish the mission.



Conclusion

The JIE is essential to bringing to bear the power of the Enterprise across the strategic, operational, and tactical levels. A standard, unified information environment is necessary to meet the operational and security requirements of modern joint military operations.

To make the vision of the JIE a reality, we must ensure that we think differently about how we deliver information technology to the warfighter. We must think enterprise first. We must embrace this new imperative and evolve the JIE to ensure secure and protected information access from every environment.

More information on JIE may be obtained from the Joint Technical Synchronization Office:
https://east.esps.disa.mil/disa/cop/jtso/SitePages/JTSO.aspx

Glossary

A –

ABCS – Army Battle Command System

ADCON – Administrative Control

ADO – Active Directory Optimization

AF – Air Force

AFNET –Air Force Network

AFSCN –Air Force Satellite Control Network

B –

B/P/C/S - Base/Post/Camp/Station

C –

C&A – Certification & Accreditation

CAC – Common Access Card

CC/S/A – Combatant Commands, Services, Agencies

CDC – Core Data Center

CIO – Chief Information Officer

CJCS – Chairman of the Joint Chiefs of Staff

COCOM – Combatant Command

CONUS – Continental United States

COP – Common Operating Picture

COOP – Continuity of Operations Plan

CYBERCOM – United States Cyber Command

D –

DCO – Defensive Cyber Operations

DCT – Device Configuration Tool

DGO - DoD Global Information Grid Operations

DECC – DISA Enterprise Computing Center

DEE – Defense Enterprise E-mail

DEPS – Defense Enterprise Portal Service

DISA – Defense Information Systems Agency

DISN – Defense Information Systems Network

DMDC – Defense Manpower Data Center

DMS – Defense Messaging System

DoD – Department of Defense

DoDI – Department of Defense Instruction

DOT&E – Director of Operational Test & Evaluation

DRSN – Defense Red Switch Network

DSN – Defense Switched Network

E –

EANCS – Enterprise-wide Access to Network and Collaboration Services

EA – Enterprise Architecture

EC – Enterprise Cloud

EDS – Enterprise Directory Services

EOC – Enterprise Operations Center

EXCOM – Executive Community

EXORD – Execution Order

F –

G –

GBS – Global Broadcast Service

GCCS – Global Command and Control System

GCSS – Global Combat Support System

GDS – Global Directory Service

GEOC – Global Enterprise Operations Center

GIG – Global Information Grid

H –

HF – High Frequency

I –

I-NOSC – Integrated Network Operations and Security Center

IA – Information Assurance

IAAS –Infrastructure as a Service

IAP – Integrated Access Point

IAW – In accordance with

IC – Intelligence Community

ICD – Initial Capabilities Document

ICS – Industrial Control Systems

IdAM – Identity and Access Management

IEA – Information Enterprise Architecture

IOT – Initial Operational Capability

IP – Internet Protocol

IT – Information Technology

ITESR – IT Enterprise Strategy and Roadmap

ITW/AA – Integrated Tactical Warning and Attack Assessment

J –

JDN – Joint Data Network

JIE – Joint Information Environment

JMC – JIE Management Construct

JOSG – JIE Operational Sponsor Group

JTSO – JIE Technical Synchronization Office

JWICS – Joint Worldwide Intelligence Communications System

K –

L –

LOS – Line of Sight

M –

MAJCOM – Major Command

MAS – Mobile Application Store

MCCC – MAGTF (Marine Air-Ground Task Force) Communications Control Center

MDA – Missile Defense Agency

MDM – Mobile Device Manager

MILDEP – Military Department

MSS – Mobile Satellite Service

MW/MD – Missile Warning / Missile Defense

N –

NGA – National Geospatial-Intelligence Agency

NIPR – Non-Classified Internet Protocol Router Network

NNT – Network Normalization and Transport

NMCI – Navy Marine Corps Intranet

NOC – Network Operations Center

NRO – National Reconnaissance Office

O –

O&M – Operations and Maintenance

OOB – Out of Band

OPCON - Operational Control

OT&E – Operational Test & Evaluation

P –

PAAS – Platform as a Service

PMO – Program Management Office

PNT - Pentagon

Q –

R –

RF – Radio Frequency

S –

SA – Situational Awareness

SAAS – Software as a Service

SAP – Special Access Programs

SATCOM – Satellite Communications

SCADA – Supervisory Control and Data Acquisition

SIPR – Secret Internet Protocol Routed Network

SOCOM – Special Operations Command

SSA – Single Security Architecture

STIG – Security Technical Implementation Guide

STO – Special Technical Operations

STRATCOM – United States Strategic Command

T –

TACON – Tactical Control

TADL – Tactical Data Link

TBMCS – Theater Battle Management Core Systems

TDM – Time-Division Multiplexing

TTP – Tactics, Techniques & Procedures

U –

U-AR – Unclassified Aggregation Router

UAV – Unmanned Aerial Vehicle

UC – Unified Capabilities

UCP – Unified Command Plan

V –

VPN – Virtual Private Network
VOIP – Voice Over Internet Protocol
VTC –Video Teleconference

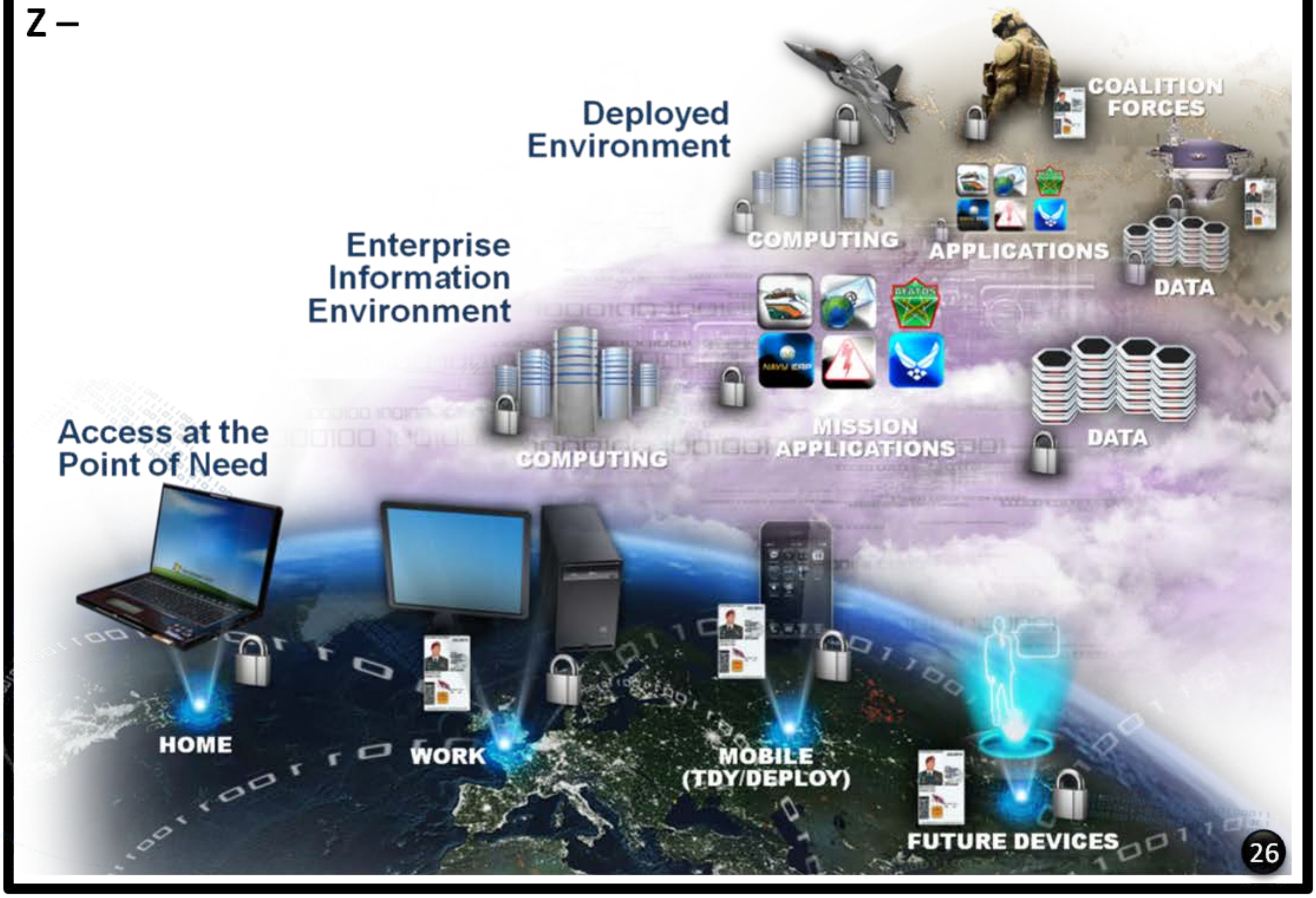
W –

WAN –Wide Area Network

X –

Y –

Z –



JIE

JOINT INFORMATION ENVIRONMENT

DISA

A COMBAT SUPPORT AGENCY

http://www.disa.mil