JITC

Joint Interoperability Test Command

Evolving the Net Ready-Key Performance Parameter

Alan Rieffer
Engineering and Policy Branch/JT4A
26 October 2011

DISA

Defense Information Systems Agency

DISA

A Combat Support Agency

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."

DISA

A Combat Support Agency

Purpose

- Present an overview of current policies and processes for assessing compliance with the Net-Ready Key Performance Parameter

- Highlight the vision, progress, and challenges in support of aligning Joint IOP TE&C with Agile development and an evolving IT acquisition model.

Goal: Establish an operationally relevant approach to Joint interoperability (IOP) engineering, test, evaluation & certification (TE&C) consistent with IT Acquisition process

DISA

A Combat Support Agency

Today: Evaluating the Net Ready KPP

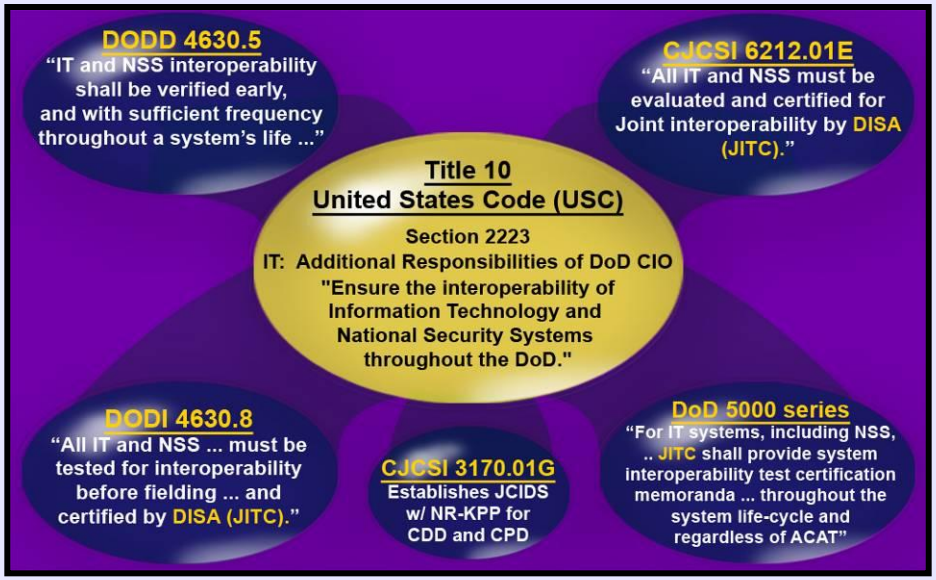
- Policies and Certification Process
- Requirements Definition
- Elements of the Net Ready Key Performance Parameter
- T&E Products and Support

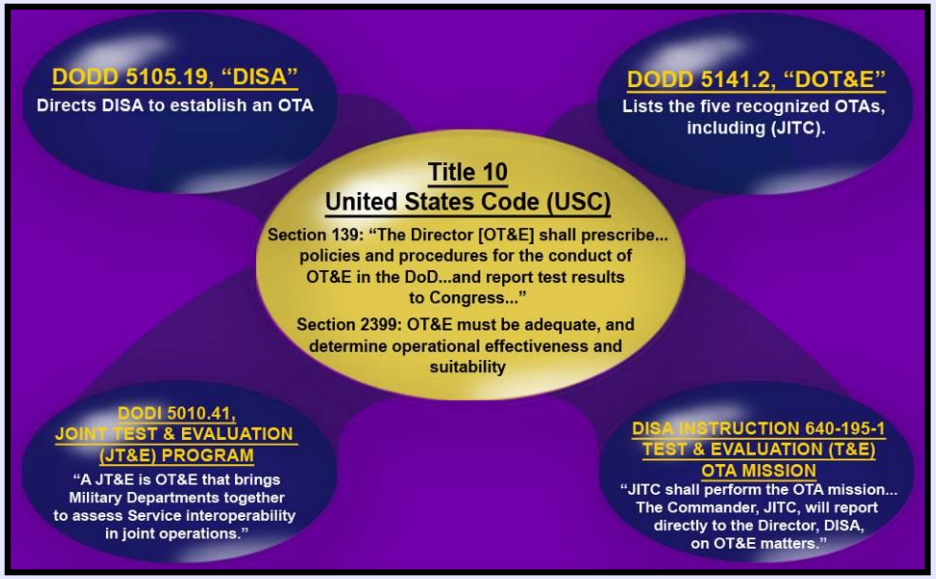
Joint Interoperability Policy

A Combat Support Agency

JS - Interoperability Certification

DOT&E - Operational Test Reports





NR-KPP T&E Process

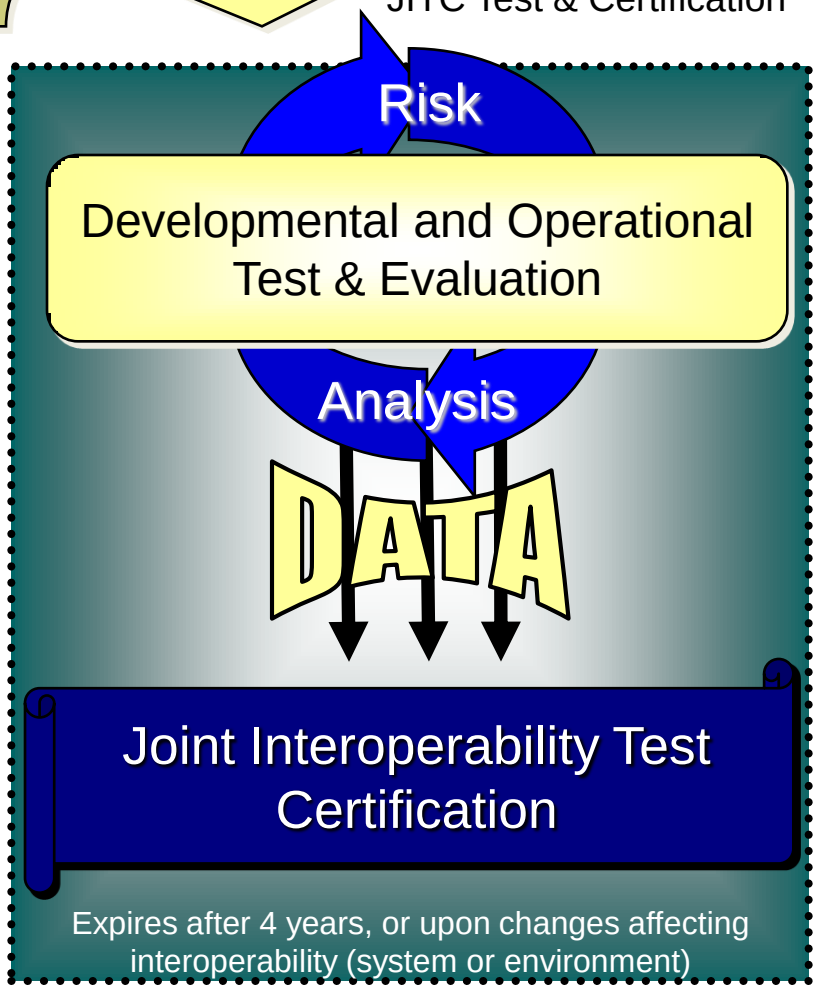
DISA
A Combat Support Agency

Joint Staff J-8

Interoperability & Supportability Certification Documents:

CDD, CPD, ISP, ISP Annex and TISP

JITC Test & Certification



NOTE: Interoperability changes require reentering process at appropriate point:

- ✓ Requirements updates
- ✓ J-8 I&S Certification
- ✓ JITC Test & Certification

DISA
A Combat Support Agency

Requirement Definition

- **Mission based requirements**
  - **Establish the operational activities and operational context**
  - **Enabled by the critical joint information/data exchanges**
  - **Drive the critical joint interfaces**
  - **Specify measures and criteria**
- **Requirements products**
  - **Reviewed by J8 for Interoperability and Supportability (I&S) Certification**
  - **Used to determine NR-KPP compliance**
  - **Threshold for certification: JS certified requirements**
    - **Information Support Plan (ISP) is preferred**

Viewpoints - CJCSI 6212.01E

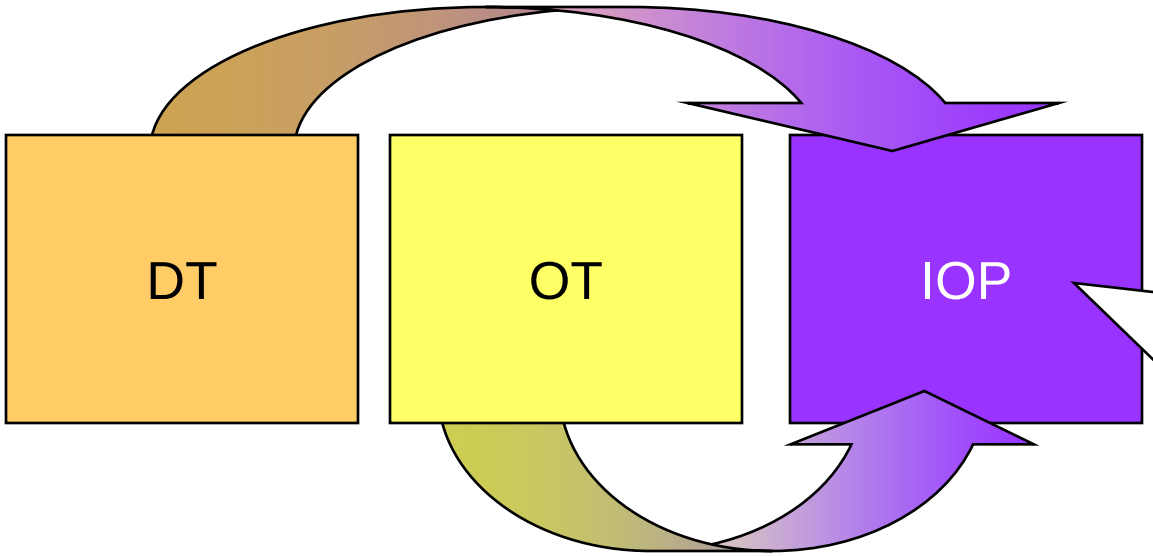
A Combat Support Agency

Document	Supportability Compliance	DOD Enterprise Architecture Products (IAW DODAF) (see Note 5)															Data/Service Exposure Sheets	IA Compliance	GTG Compliance
		AV-1 /AV-2	OV-1	OV-2	OV-3	OV-4	OV-5	OV-6C	OV-7	SV-1	SV-2	SV-4	SV-5	SV-6	SV-11	TV-1	TV-2			
ICD			X																	
CDD	X	3	X	X	X	X	X	X			X	X	X	X		2	2	1	X	X
CPD	X	3	X	X	X	X	X	X	1		X	X	X	X	1	2	2	1	X	X
ISP	X	3	X	X	X	X	X	X	4		X	X	X	X	4	2	2	1	X	X
TISP	X	3	X		X		X	X		X			X	X		2	2	1	X	X
ISP Annex (Svcs/ Apps)	X	3	X				X				X	X	X	X		2	2	1	X	X
X		Required (PM needs to check with their Component for any additional architectural/regulatory requirements for CDDs, CPDs, ISPs/TISPs. (e.g., HQDA requires the SV-10c)																		
Note 1		Required only when IT and NSS collects, processes, or uses any shared data or when IT and NSS exposes, consumes or implements shared services,																		
Note 2		The TV-1 and TV-2 are built using the DISRonline and must be posted for compliance.																		
Note 3		The AV-1 must be uploaded onto DARS and must be registered in DARS for compliance																		
Note 4		Only required for Milestone C, if applicable (see Note 1)																		
Note 5		The naming of the architecture views is expected to change with the release of DODAF v2.0 (e.g., StdV, SvcV, StdV, DIV). The requirements of this matrix will not change.																		

DARS= DoD Architecture Registry System

DISA
A Combat Support Agency

Joint Interoperability Test Certification



NR-KPP Elements:

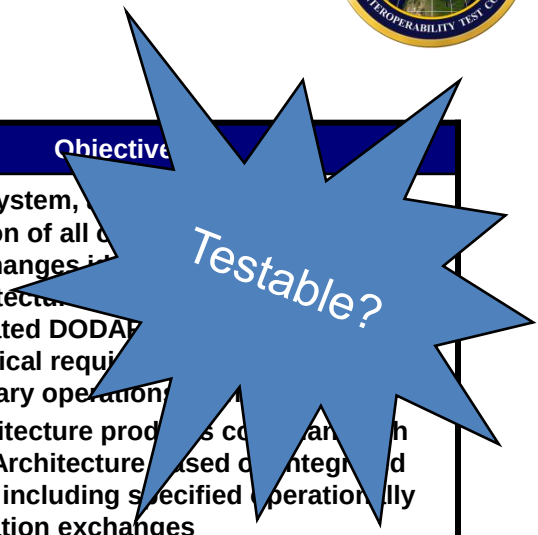
- Compliant Solution Architectures
- Net-Centric Data and Services Strategy
- GIG Technical Guidance
- Information Assurance
- Supportability

- **The NR-KPP elements define the areas JITC evaluates for interoperability certification**
- **JITC uses data collected during DT, OT, demonstrations, exercises, or other reliable sources for interoperability evaluations**

Success = Minimizing separate interoperability testing by leveraging DT/OT

NR-KPP Statement

DISA
A Combat Support Agency



KPP	Threshold	Objective
Net-Ready: The capability, system, and/or service must support Net-Centric military operations. The capability, system, and/or service must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The capability, system, and/or service must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.	The capability, system, and/or service must fully support execution of joint critical operational activities and information exchanges identified in the DoD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization to Operate by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.	The capability, system, [illegible] support execution of all [illegible] information exchanges [illegible] Enterprise Architectu[illegible] based on integrated DODA[illegible] satisfy the technical requi[illegible] Net-Centric military operation[illegible] 1) Solution architecture prod[illegible]s co[illegible]an[illegible]h DoD Enterprise Architecture[illegible]ased o[illegible]ntegr[illegible]d DODAF content, including s[illegible]ecified [illegible]peration[illegible]lly effective information exchanges 2) Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization to Operate by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.

DISA

A Combat Support Agency

NR-KPP Elements

- **Compliant 'Solution Architectures'**
  - **Demonstrate operationally effective information exchanges**
- **Net-Centric Data and Services Strategy Compliance**
  - **Data & Services; DoD Information Enterprise Architecture (IEA)**
- **Global Information Grid Technical Guidance**
  - **Compliance as required by DoD Enterprise Architecture and Solution Architectures**
- **Information Assurance**
  - **IATO or ATO issued by Designated Approval Authority (DAA)**
  - **Test production-representative, IA approved configuration**
- **Supportability**
  - **Miscellaneous requirements: GPS Selective Anti-Spoofing, spectrum compliance, Joint Tactical Radio implementation**

NR-KPP Statement Provides a Framework for Evaluation

DISA
A Combat Support Agency

Solution Architectures
Criteria

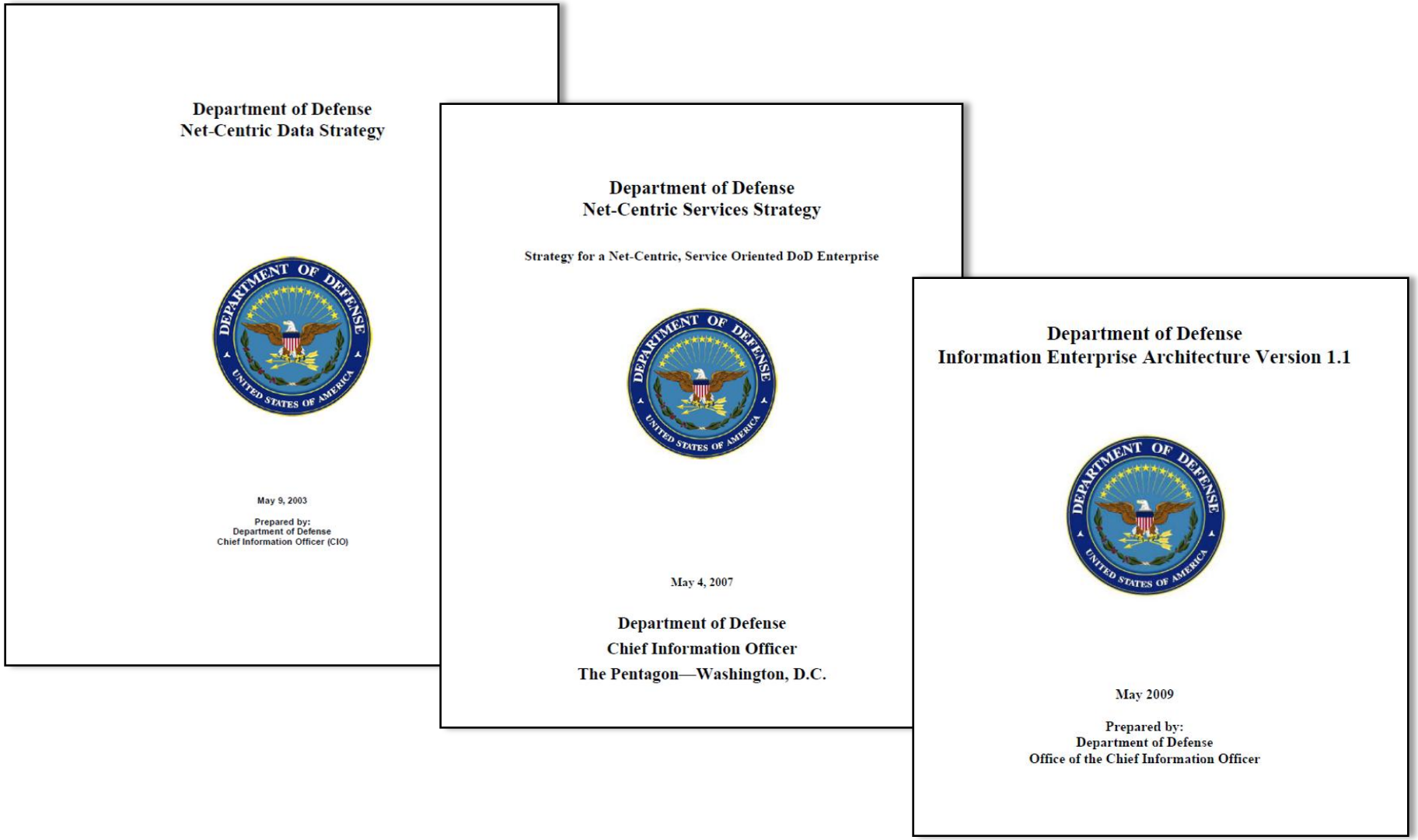
- **Demonstrate operationally effective IE's**
  - **Threshold: all *JOINT CRITICAL* information exchanges***
  - **Objective: *ALL* information exchanges***

    *** Requirements contained in certified ISP CDD, etc.**
- **Joint Critical: defined as *any* operational activity or Information Exchange (IE) designated as critical in Joint Staff-certified requirements documents**
- **Information and data exchange requirement attributes and interfaces are explicitly defined in:**
  - **OV-3 Information Exchange Matrix, and**
  - **SV-6 System Data Exchange Matrix**

DISA
A Combat Support Agency

Data and Services Strategy

Requirements Sources



DISA
A Combat Support Agency

Data and Services Strategy

Requirements Breakout

Net-Centric Data Sharing Requirements
Data is Visible: Post discovery metadata in an Enterprise Catalog Use appropriate keywords for discovery
Data is Accessible: Post data to shared space Provide access policy Provide serving (access) mechanism Publish active link to data asset
Data is Understandable: Publish semantic and structural metadata Register data artifacts in DoD MDR
Data is Interoperable: Base vocabularies on Universal Core (UCore) Comply with COI data-sharing agreements Conform to DDMS
Data is Trusted: Provide information assurance and security metadata

Net-Centric Service Sharing Requirements
Services are Visible: Publish a description of the service or access mechanism Comply with enterprise-specified minimum service discovery requirements
Services are Accessible: Provide an active link to the service in the enterprise catalog Provide an active link to the service in the NCES Service Registry
Services are Understandable: Publish a description of the service or access mechanism to the NCES Service Registry Publish service artifacts to Provide NetOps Data (NetOps Agility) DoD MDR Provide service specification or Service Level Agreement (SLA)
Services are Trusted: Operate services in accordance with SLA Include security mechanisms or restrictions in the service specification Enable continuity of operations and disaster recovery for services Provide NetOps Data (NetOps Agility)
Use of Core Enterprise Services (CES): Core Enterprise Services (CES) are used in accordance with DoD CIO mandates

Data Visibility Example

A Combat Support Agency

Net-Centric Data Sharing Requirements
Data is Visible: Post discovery metadata in an Enterprise Catalog Use appropriate keywords for discovery
Data is Accessible: Post data to shared space Provide access policy Provide serving (access) mechanism Publish active link to data asset
Data is Understandable: Publish semantic and structural metadata Register data artifacts in DoD MDR
Data is Interoperable: Base vocabularies on Universal Core (UCore) Comply with COI data-sharing agreements Conform to DDMS
Data is Trusted: Provide information assurance and security metadata

- **Data Visibility criteria**
  - **Discovery metadata (DMD) visible in a shared space, i.e., NCES Enterprise Catalog or DCGS DIB**
  - **DMD DDMS compliant**
  - **Discovery keywords appropriate for mission area or data type**

DISA
A Combat Support Agency

Data and Services Strategy

Criteria

- **Threshold**: Demonstrate ability to exchange information for **all Joint Critical exchanges** and that the **data assets and services** required to support those exchanges **meet the net-centric requirements** for data and services (i.e. visibility, accessibility, etc.)
- Objective: Demonstrate ability to exchange information for ALL exchanges and that the data assets and services required to support those exchanges meet the net-centric requirements for data and services (i.e. visibility, accessibility, etc.)

DISA
A Combat Support Agency

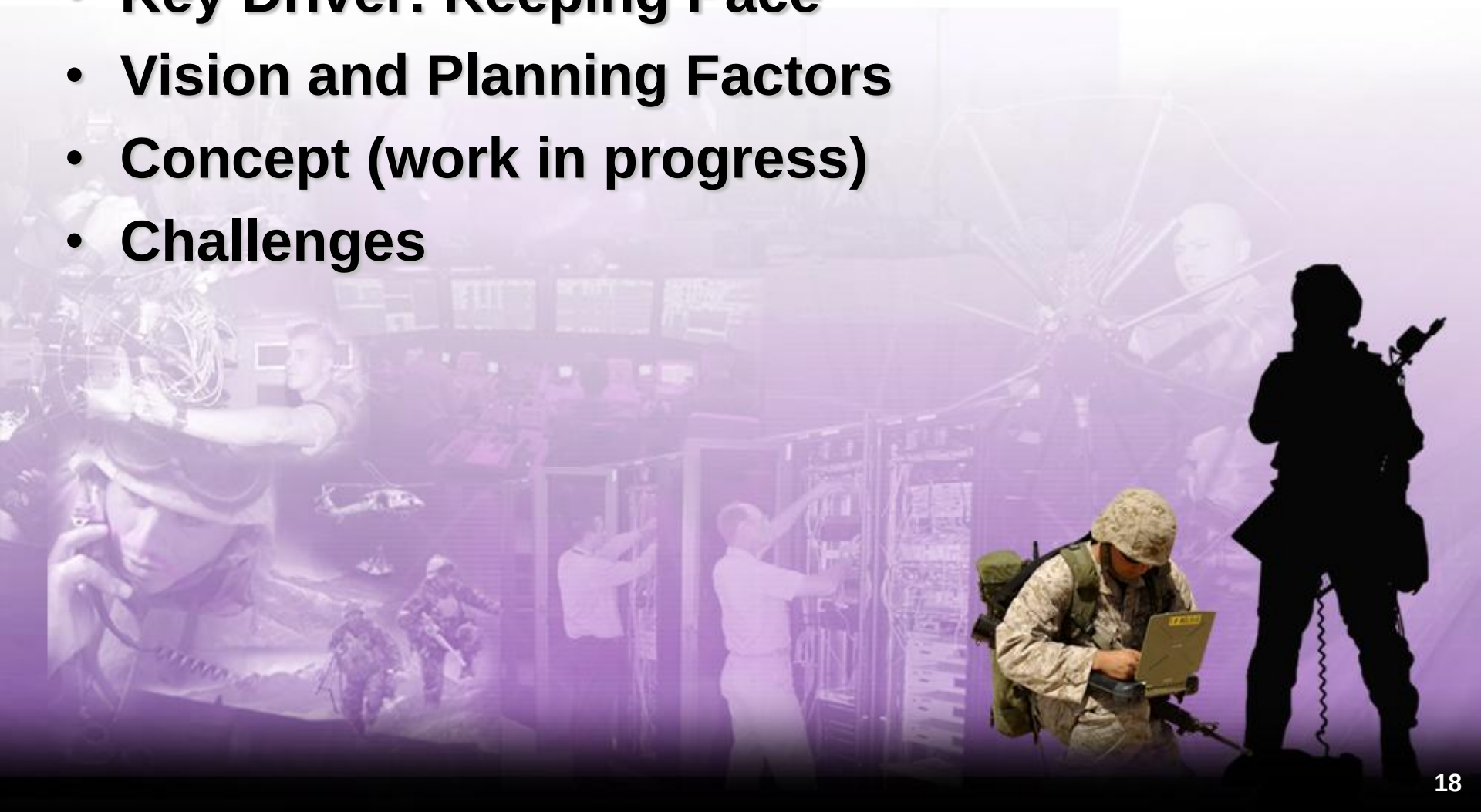
Interoperability Certification Products

Certification	Description	System can be fielded (Y/N)?
Standards Conformance Certification	System is certified for conformance to a standard/ standards profile	No
Joint Interoperability Test Certification	Full system certification. System meets at least ***all critical*** interoperability requirements	Yes
Limited Joint Interoperability Test Certification	System meets ***subset*** of critical interoperability requirements	Yes, with ICTO
Interim Joint Interoperability Test Certification	A capability module has adequately demonstrated interoperability for at least ***all critical*** threshold requirements identified for the increment	Yes
Special Interoperability Test Certification	Certification is based on other J-8 approved requirements other than the NR-KPP, e.g., use of UCR for voice switches	Yes
Non-Certification	Critical operational impacts expected Provides a warning to the warfighter	No
Interoperability Assessment	PM would like to determine interoperability status. System may lack J-8 certified requirements	No

DISA
A Combat Support Agency

Emerging: Aligning TE&C with Agile Development

- Key Driver: Keeping Pace
- Vision and Planning Factors
- Concept (work in progress)
- Challenges

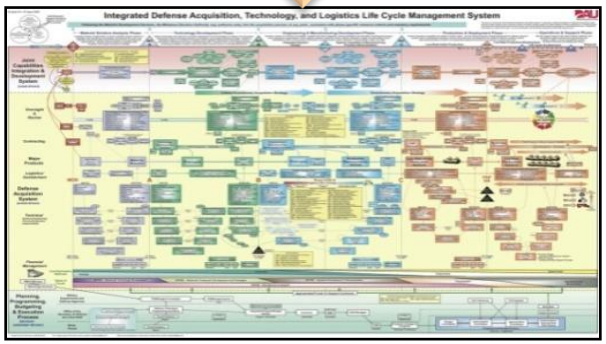


Key Driver: Keeping Pace

A Combat Support Agency

Weapon System

- Weapon platform centric
- Requirements 'well' defined and locked before developing
- New or unique technologies
- Development cycle in years
- Formal production decisions
- Service lives extending into decades



IT System

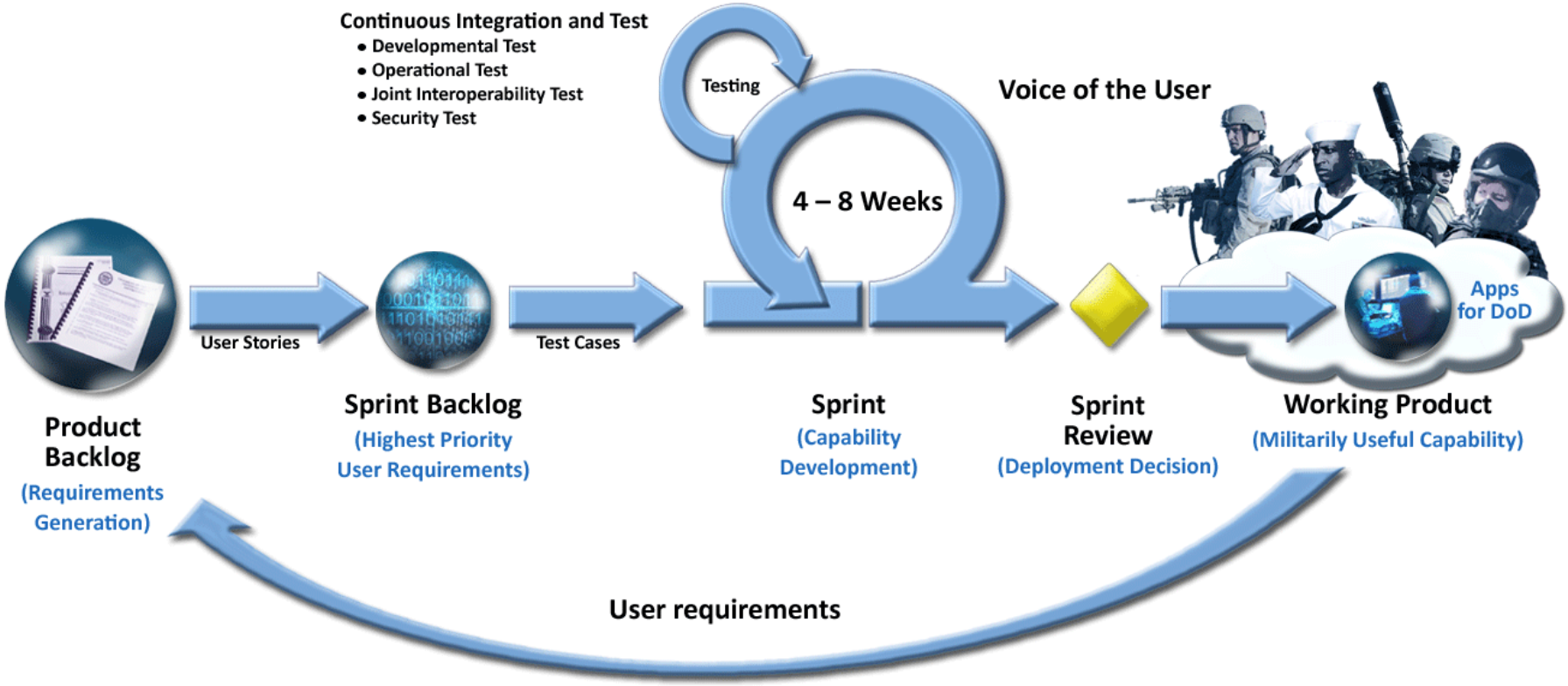
- Application based capability (SW intensive)
- Existing 'Stable' Enterprise (not static)
- Network Centric
- Employ existing technologies
- Build-field cycle 12-18 months
- Commodity H/W & Computing
- Periodic technology refresh to avoid obsolescence

Need Integrated TE&C Processes to support DoD Acquisition Process Optimized for S/W Intensive IT Systems

Vision: Test Transformation

Supporting IT Acquisition Reform

A Combat Support Agency



* Sprint is used here as a name for smallest increment of deployable software

IT Acquisition Reform Supported by Agile Test, Evaluation, and Certification

Vision: Test Transformation

DISA
A Combat Support Agency

Provisioning integrated services across acquisition processes and life-cycle

Requirements

CJCSI 3170.01G – JCIDS

CBA → JMTs → ICD → MDD → CDD → Updates

CJCSI 6212.01E - I&S Process

JMT / ICD Validation

CDD / ISP Helpdesk

Initial ISP → Updates

Responsive Requirements Process

COCOMs

FCB

Acquisition

DoD 5000 Series – Defense Acquisition System

DISA T&E

Agile Test and Evaluation

Architecture Helpdesk

Business Analysis → MS → Architecture Development → Solution Architecture → MS → Requirements → Backlog → Sprint → Decision

Apps for DoD

Working Product

Infrastructure

DoDI 3200.11 - Major Range and Test Facility Base

Infrastructure Improvement and Provisioning

GIG Services, Networks, Instrumentation, M&S and other T&E Infrastructure

Responsive & Representative Infrastructure

Making Acquisition Processes and Infrastructure Responsive to the Warfighter

DISA
A Combat Support Agency

Planning Factors
for IOP Test Certification Process

- **Guiding principles**
  - **OSD Report to Congress (Dec 2010)**
  - **US Chief Information Officer (Nov 2010)**
- **Mission Based; provide operational impact**
- **What questions really need to be answered?**
- **Applicability (Agile developed capabilities)**
  - **Focus on Enterprise Service and Application IOP**
- **Risk based test strategy**
- **Support the IT Acquisition Model (evolving)**
  - **Converging requirements, capabilities, and testing**
- **Scope: joint interoperability**

Incremental TE&C Concept

DISA
A Combat Support Agency

ACTIVITIES

Backlog Refinement
- Initial Reqmts Definition
- Release Planning
- Risk Analysis
- IOP Test Scope ID

Sprint Planning
- Proposed Capabilities & Acceptance Criteria
- Risk Analysis
- Test Strategy
- Infrastructure

Sprint Timebox
- Develop, Test & Data Collect
- Data Reduction & Analysis
- Refine, Adjudicate, and Document IOP Requirements
- Update Test Strategy
- Assess Status of IOP and Operational Impact (risk)

Sprint Review
- IOP Requirements are updated
  - Digitally captured
  - Approved (If applicable)
- Update Status of IOP (e.g. Assessment)
- Draft Applicable IOP Certification Memo

CONVERGENCE
Capabilities
Requirements
Test Results
CERTIFICATION OR FIELDING DECISION

4 – 8 Weeks

User Stories

Test Cases

Product Backlog (PB)

Sprint Planning (SP)

Sprint

Sprint Review (SR)

PB Artifacts
- **IOP T&E Strategy**
  - Applicable IOP elements
  - Applicable PB items
  - IOP Testing Scope
- **IOP Evaluation Structure**
  - Mission
  - Activities
  - KPPs
  - Functions
  - IERs

Sprint Planning Artifacts
- **IOP T&E Strategy**
  - Data collection strategy/list
  - Standards conformance testing
  - IA coordination
  - DSS
- **IOP Evaluation Structure**
  - DERs
  - Standards reqmts
  - IA
  - Config Mngmt reqmts
  - DSS
  - Sample Size
  - Metrics

Sprint Artifacts
- **IOP Evaluation Structure (refined)**
  - Updated requirements
  - Test Results
  - IA
  - Automated Test Results (conformance)

Sprint Review Artifacts
- **IOP Test Results**
- **IOP Status ***
- Approved Requirements
- Capabilities – Risks
- Fielding Recommendation
- **IOP Cert Memo**

*** As applicable**

ARTIFACTS

Requirements Evolution Example

DISA
A Combat Support Agency

Top-level Requirements - Joint Staff Approved

- Overview and Summary Information
- High-Level Operational Concept
- Operational Activities

Top-level Requirements Approved by Joint Staff J8

Sprints

- User Stories
- Product Backlog

Drives detailed functionality/information exchange requirements over time within the bounds of approved requirements

Derived, Detailed Requirements Approved by lower-level authority

Mediated by overarching requirements (e.g., standards, architectures, JMTs, COI requirements, etc)

- Joint Task & Mission Thread Information
- System Interface(s) & Services Functional Descriptions
- Detailed System & Services Data Exchange Requirements

Derived requirements through Agile development processes

Requirements Evolution Example

DISA
A Combat Support Agency

	Product Backlog Refinement	Sprint Planning	Sprint Cycles	Sprint Review	Fielding Decision
Elements of IOP	Initial Agile Requirements	Executable User Stories	Requirement Refinement (Sprints 1-n)	Lockdown S/W & Req's; Sprint Results	Reqs Cert for Fielding or IOP Cert
Op Effective Information Exchanges	Entry Level (AV-1, OV-1, OV-5 like)	Evolve Initial IER and LLEE	Capabilities & Requirements converge	Locked, Assess based on Sprints	**Req's** **Certified**
Data,Services Net Entry	Evolving	Support Sprint Cycle	Enterprise int	Locked, Assess	**for**
Standards & Specs-GTG	Evolving	Evolving	Automated tests	Locked, Assess	**S/W**
Info Assurance	Evolving	Evolving	TBD	Locked, Assess (IATO?)	**Release**
Supporting Docs	Evolving	Evolving	Light weight, test driven	Objective Evidence	Tracks w/ Capability

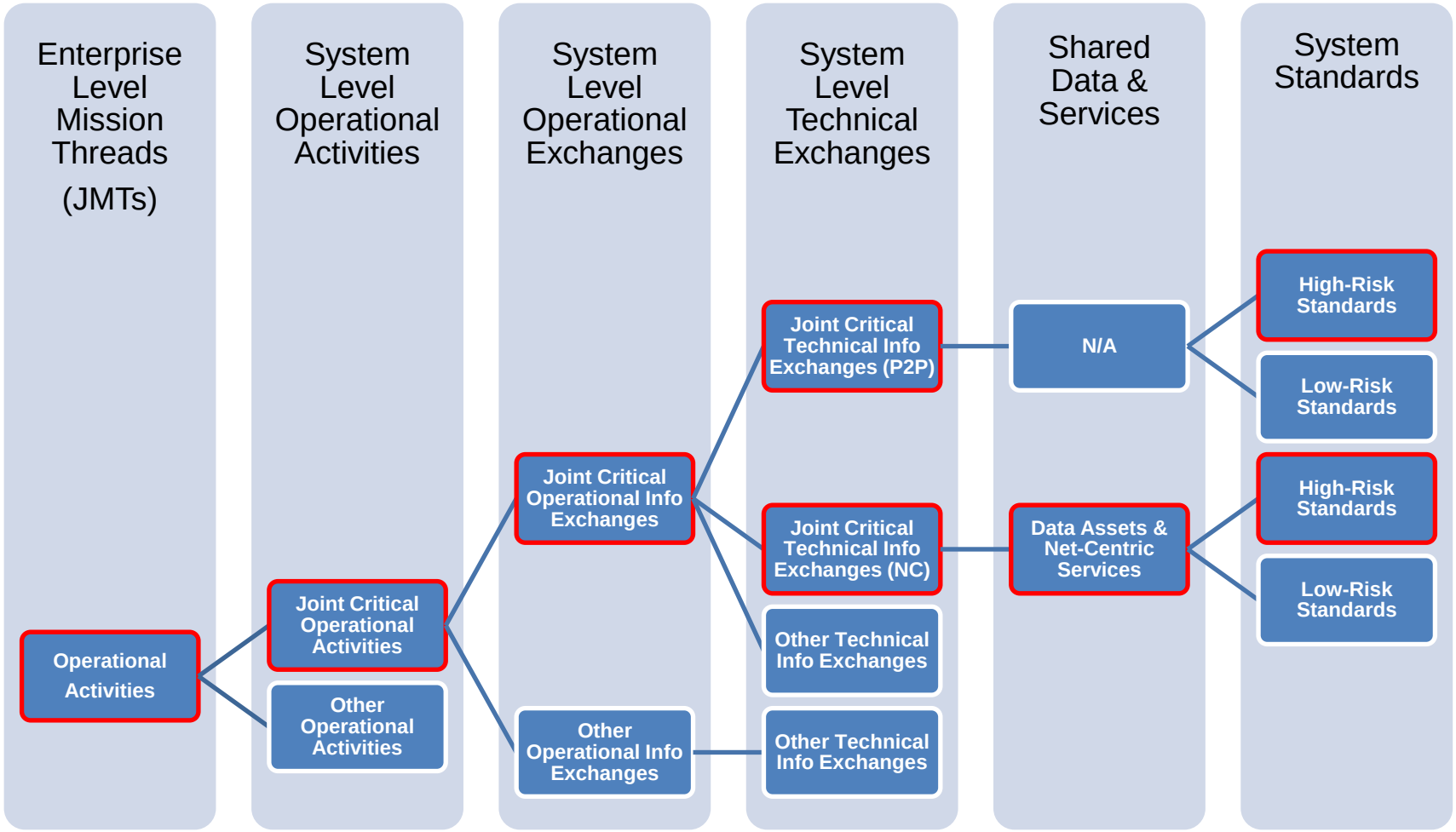
Notional Example

Agile Requirements Evolution
(Detail Typically in ISP)

Delegate requirement approval authority for IER implementation and other critical technical parameters if consistent with approved operational activities

Balance Risk; Understand Operational Impact

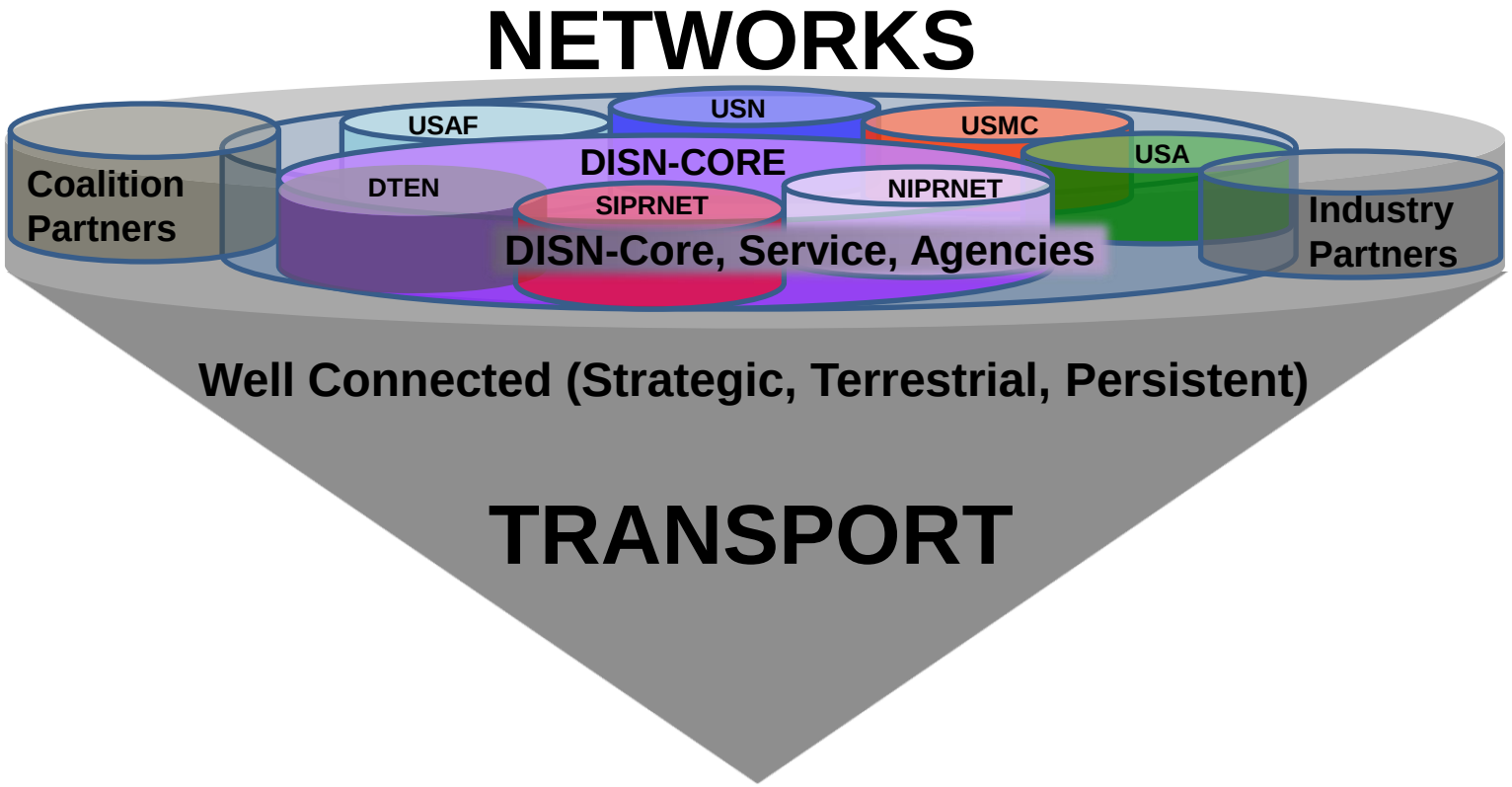
DISA
A Combat Support Agency



DISA

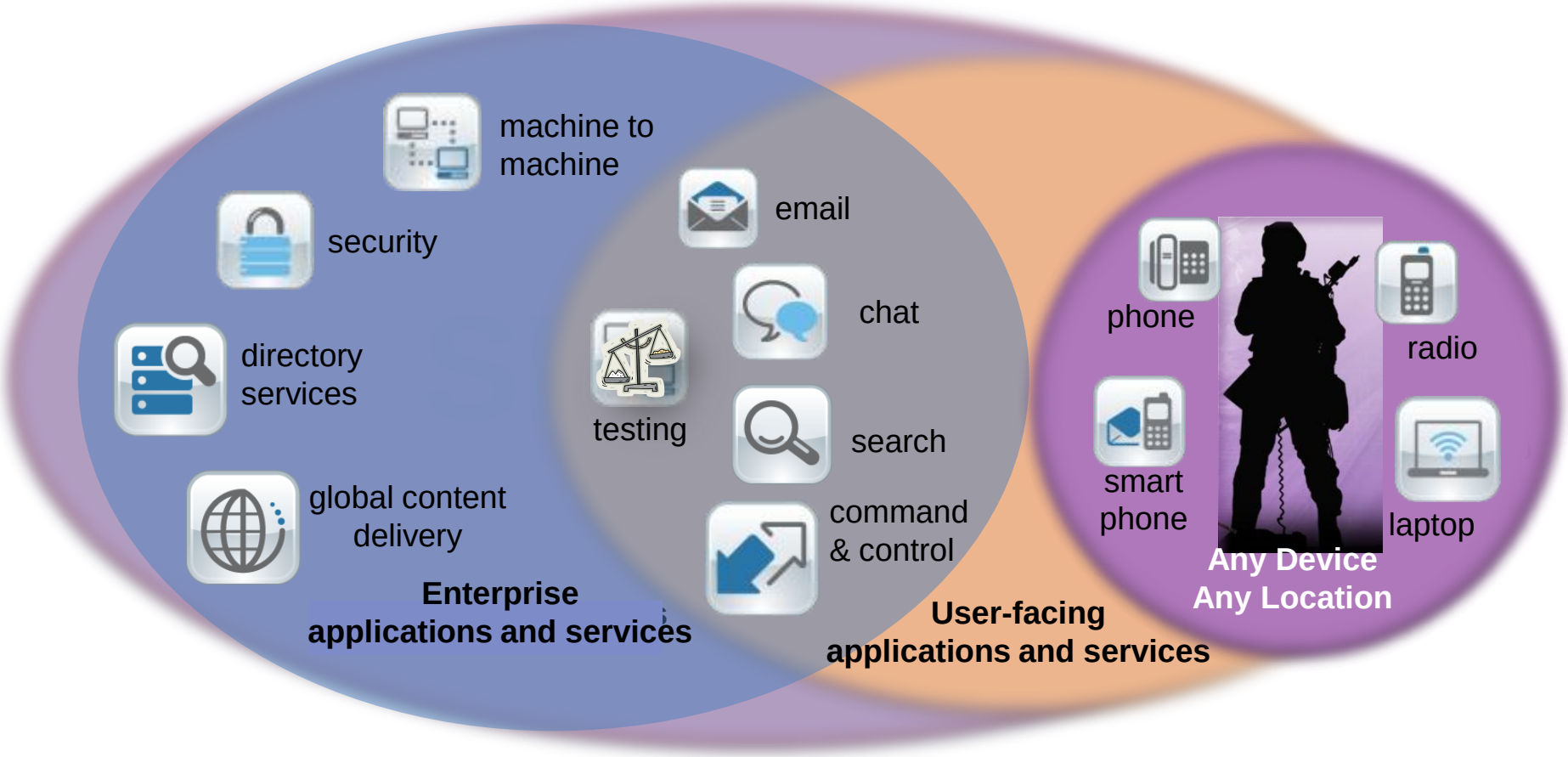
A Combat Support Agency

Provision Persistent Test Enterprise



Provision Persistent Test Enterprise

DISA
A Combat Support Agency



Enterprise Services Enable End-to-End Joint Information Sharing

DISA
A Combat Support Agency

Challenges

- **Process development & policy alignment**
  - **IT Acquisition process; Governance (oversight)**
  - **Requirements & certification processes; Independence**
- **Budgeting - Funding**
  - **Evolving requirements**
  - **Early involvement, integrated team (design, develop, test)**
- **Education**
  - **Culture & mindset for new IT acquisition processes**
  - **Integrated TE&C processes & technical skill sets**
- **Provisioned test environment**
  - **Federated test enterprise; persistence; automation**
  - **Operationally relevant; testing as a service**
- **Others TBD…**

Resources and References


DEFENSE INFORMATION SYSTEMS AGENCY