DoD Information Enterprise Architecture (IEA) Version 3.0

Briefing to DON IT Conference

DoD CIO Architecture and Engineering Directorate

22 February 2017

Overview of the Plan

- Background:
  - The DoD IEA consists of two tiers:
    - Tier 1: Top-level IEA document
    - Tier 2: EASB-approved Reference Architectures
  - Initiated development of DoD IEA v3.0 (Tier I) in June 2014
    - Focused on merging the approved versions of the DoD IEA v2.0 and the JIE EA v0.4
    - Developed draft versions of the AV-1, OV-1, CV-1, and CV-2
    - Ceased work on the DoD IEA v3.0 (Tier I) in October 2014 due to changing priorities and needs
  - Directed to re-initiate development and complete DoD IEA v3.0
- Way Ahead:
  - Establish Tiger Team (TT) from Services and other DoD Components to develop the DoD IEA v3; solicited EAEP member volunteers to be part of TT at 11 Jan 2017 EAEP meeting
  - Re-initiate development of DoD IEA v3
  - EAEP Secretariat will facilitate development
  - EASB is the approval authority for the DoD IEA v3

Things to Consider During Development

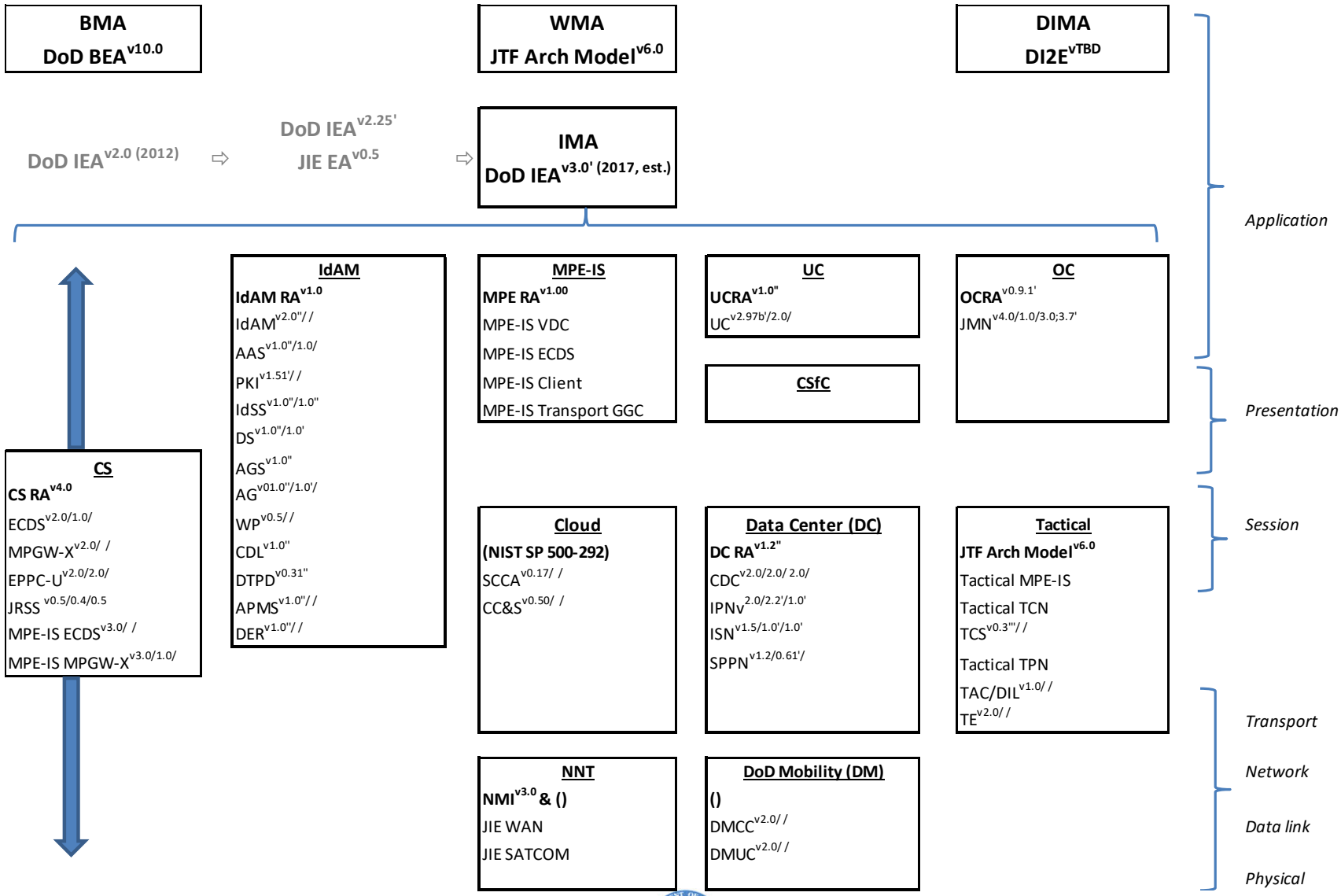
- DoD IEA v3 needs to be purpose driven by the intended uses. Broadly:
  - Downward: Provides design guidance for solutions
  - Upward: Justifies solution resource requirements in terms of strategies, missions, capability requirements, and threats
    - Focus on supporting JIE implementation and investment analysis
  - Mechanisms: Invoked by policies, e.g., JCIDS, DAS, Interoperability, JIE, … (see next slide)
- Need to integrate / align / synchronize existing Tier 2 RA's with Tier 1 development
- Potential foundational and strategic documents that guide, constrain, and inform the DoD IEA include:
  - Strategic:
    - DoD Information Technology Environment Way Forward
  - DoD Foundational:
    - Joint Capability Areas
    - Universal Joint Task List
    - Joint Common Systems Function List
  - DoD Information Mission Area (IMA):
    - JIE ICD
    - JIE CONOPS
    - JFHQ-DoDIN CONOPS
    - JP 3-12(R)(Cyberspace Operations
    - DESMF / ITIL
  - DoD Information Mission Area (IMA):
    - JIE ICD
    - JIE CONOPS
    - JFHQ-DoDIN CONOPS
    - JP 3-12(R)(Cyberspace Operations
    - DESMF / ITIL

Possible Uses Worksheet Format

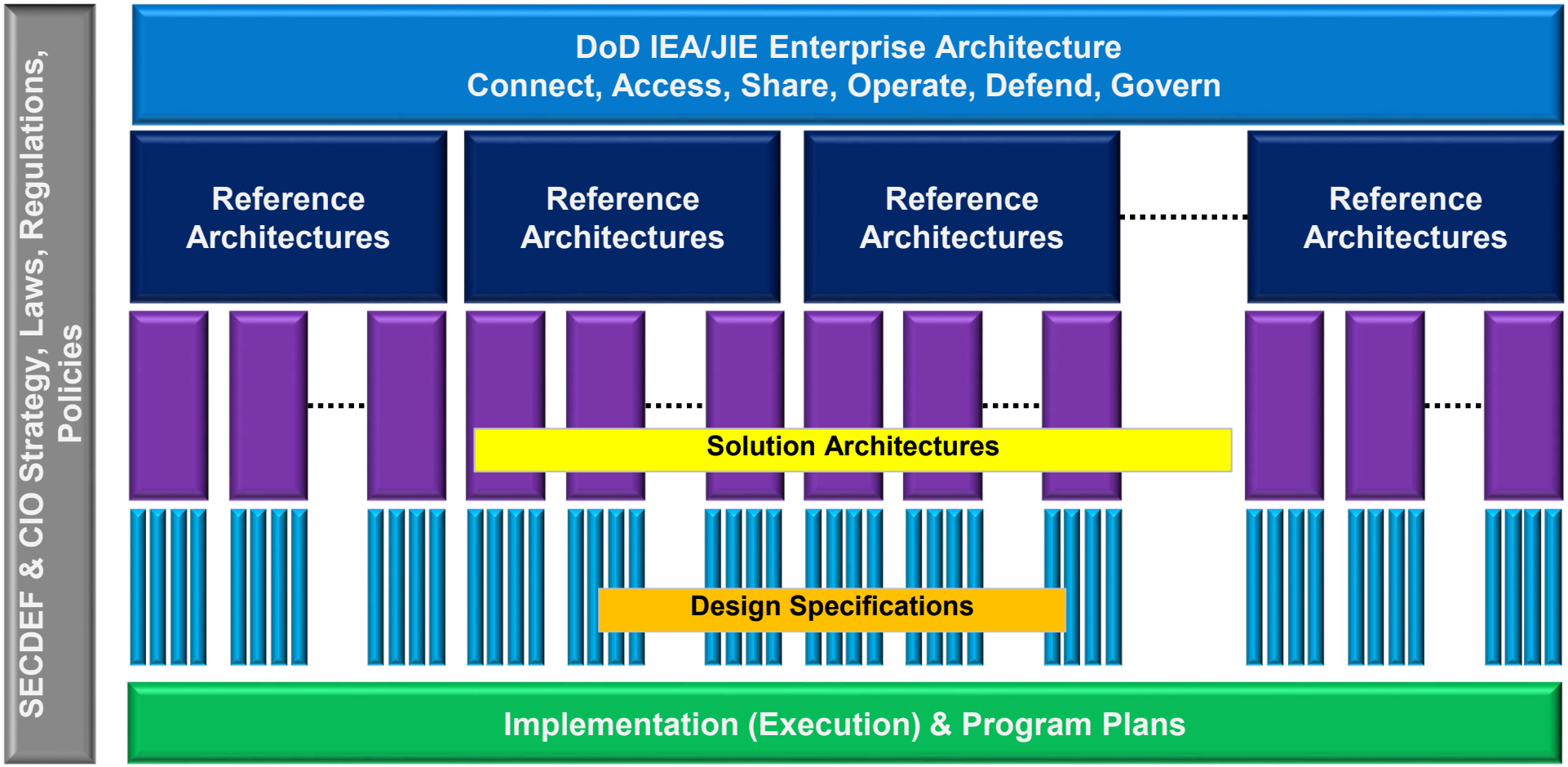
Driver	Summary	Possible Role IEA Plays
DoD IT Environment Way Forward	Vision for future IT Environment	Provides line-of-sight from strategies to IE architectures.
Enterprise Architecture and Services Board (EASB)	Approves all IMA architectures and promulgates them to DoD Components via memo.	a. DoD IEA is a one-stop-shop for approved architecture baseline b. DoD IEA aligns all approved architectures
JIE DoDI (in-progress)	Policy on JIE	The DoD IEA includes the JIE architecture
DoDI 8270.bb, DoD Architecture (in-progress)	One-stop-shop for all DoD architecture policies	a.
CJCSI 3170, JCIDS	Capabilities assessments, descriptions, and development processes, aligned with DAS.	a. Provides standard top-level terminology for ICD, CDD, and CPD IE Capabilities, Activities, Measures, … b. Guidance for CBA and ICD development to consider to-be IE Capabilities c. Guidance for evolution of IMA portions of JCSFL
DoDD/I 5000.02, DAS	Requirements for DoD acquisition in terms of process and data.	Criteria for technical review for MS and SETRs: program information architecture should be compatible for IEA for the time-frame of the program
DoDI 8330.01, Interoperability of IT and NSS	Applies to all DoD IT and NSS throughout life-cycle	Alignment with DoD IEA is a criterion for interoperability
DoDI 8000.01, DoD IE	Alignment of DoD Component IT activities.	DoD IEA is the alignment yardstick
DoDI 8500.01, Cybersecurity DoDI 8510.01, RMF DoDI 8530.01, Cybersecurity Activities	Policies for assuring cybersecurity in DoD IT an NSS	DoD IEA provides high-level cybersecurity and IdAM architectures to which solutions align.
DoDI 8115.01, IT Portfolio Mgmt	IT investments management	Investments align to DoD IEA
others		

Additional columns as needed

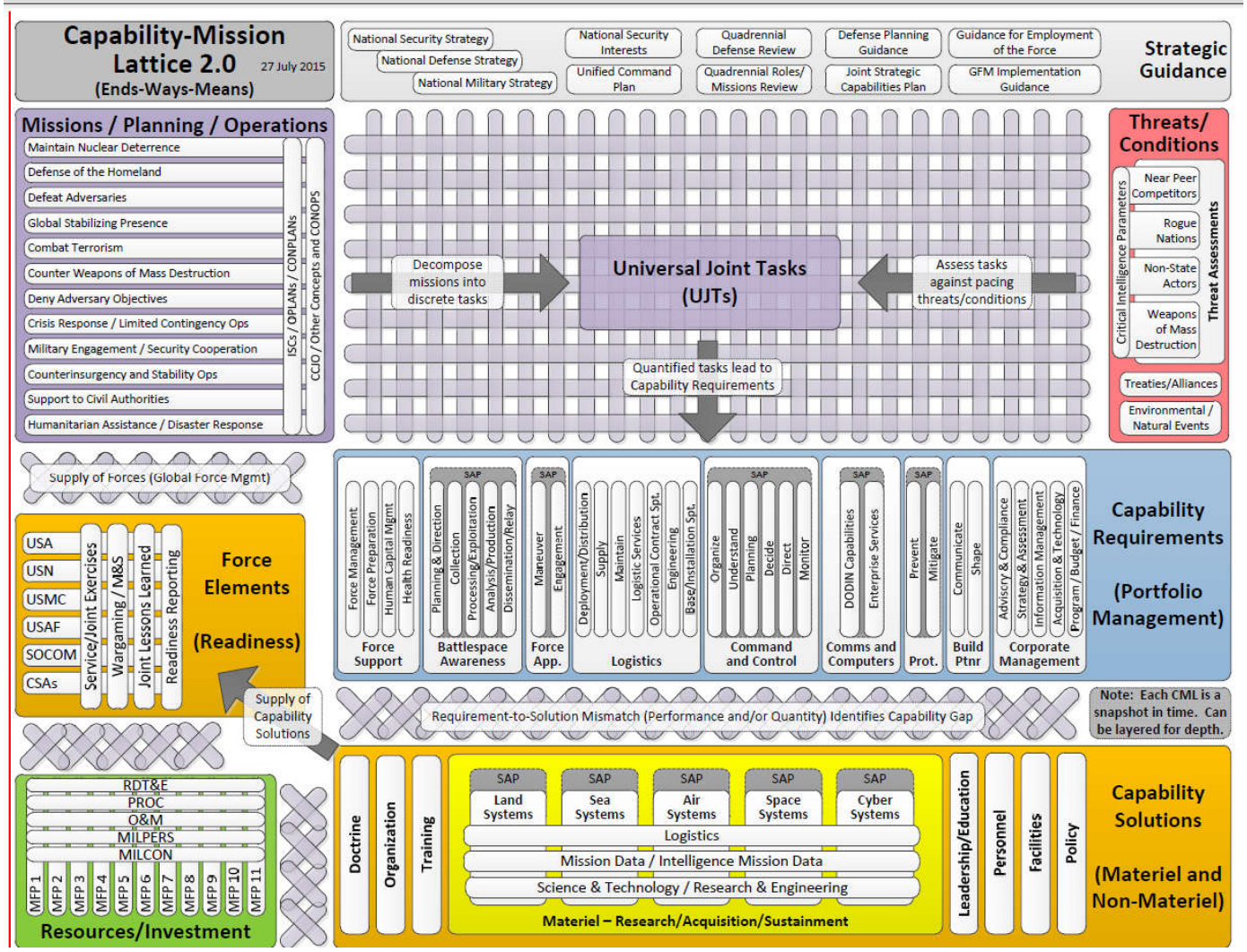
Tier 1 and Tier 2 Relationship



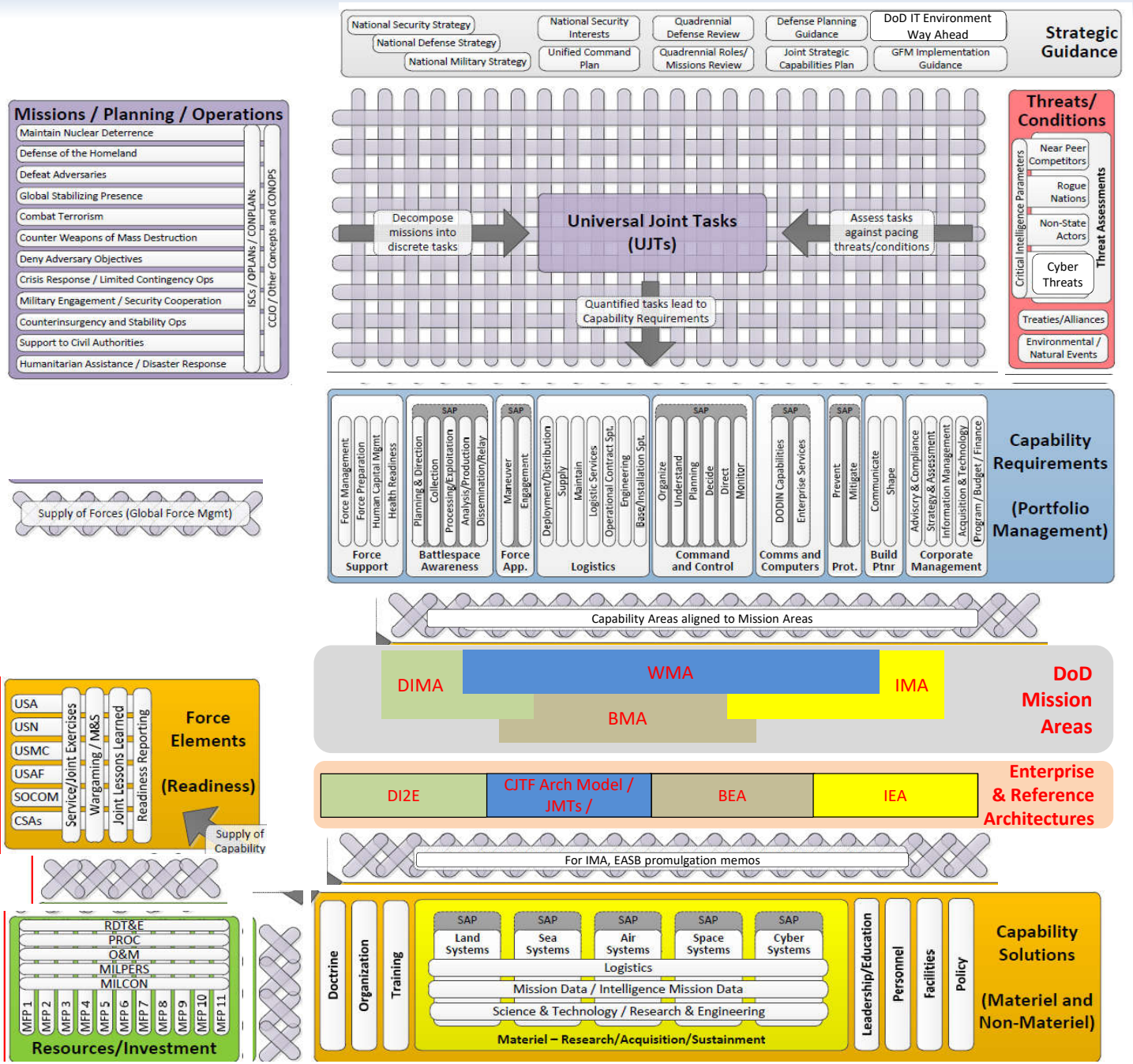
Linking and Aligning



Alignment Pattern: JCIDS Manual Capability Mission Lattice



CML and DoD IEA v3.0



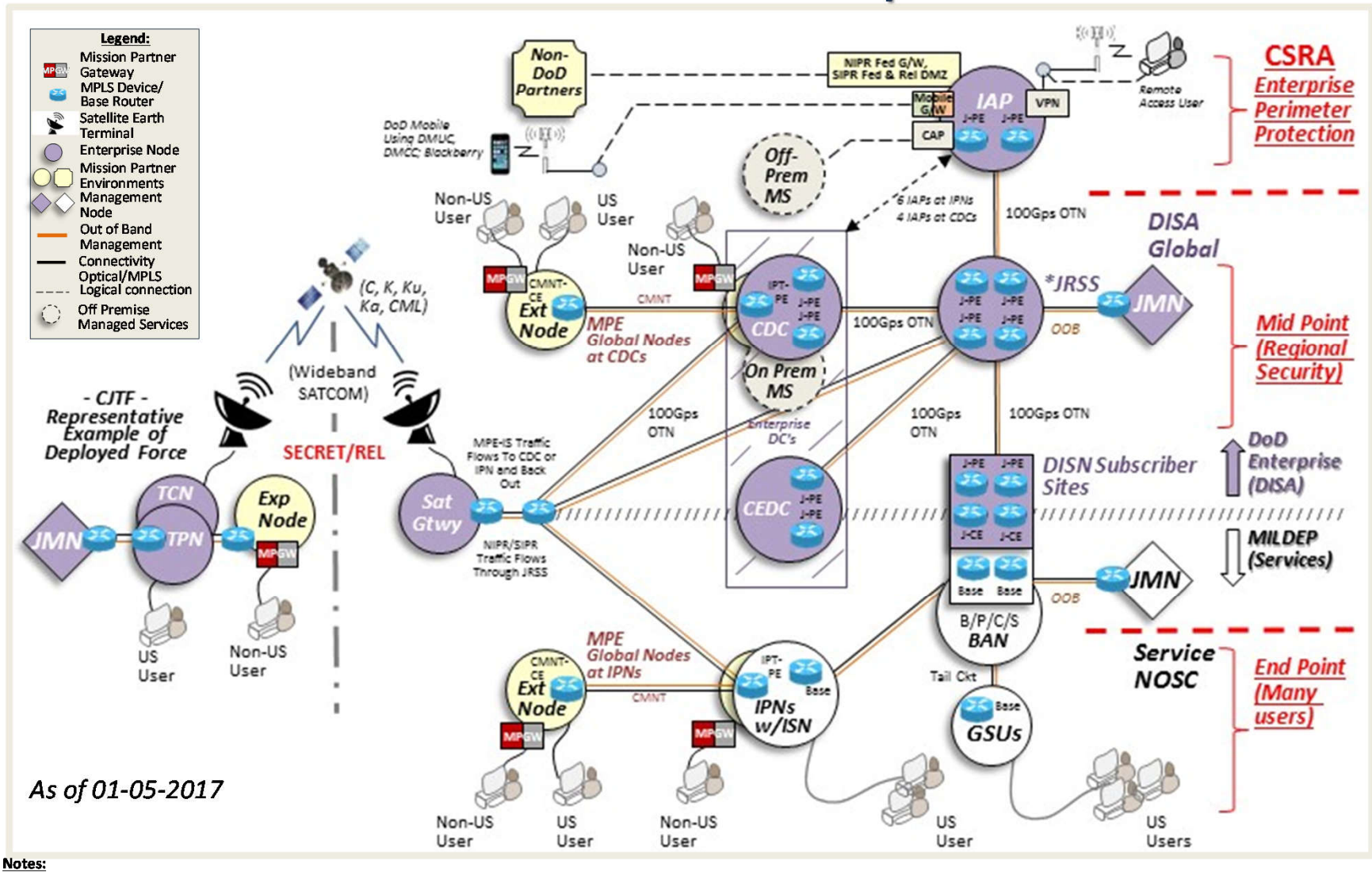
Projected High-Level Tasks Schedule

Task(s)	Timeline
Initial planning & scoping	Jan – Feb 2017
Determine uses of DoD IEA v3 with process stakeholders	Feb 2017 – Throughout Development
Verify Mission Areas (MAs) and IE capability requirements	Feb 2017
Determine traceability requirements to Foundational and Strategic guidance	Feb 2017
Determine data / artifacts that need to be synchronized across Tier 1 and 2	Mar 2017
Refine data in collaboration with MAs and RA developers	Apr -- Jun 2017
Produce Draft Architecture Report and Model	Jun – Aug 2017
Finalize document and models for coordination	Aug 2017
Coordinate all views with EAEP (Review & Assessment) and make final edits	Aug – Oct 2017
EASB Approval	Oct 2017

Questions and Comments?

JIE Nodal Topology (SV-1/2)

Fit for Purpose



DESCRIPTION

The JIE Framework SV-1/2 represents the end-to-end (tactical edge war-fighter's communications connectivity to the sustaining base Infrastructure) in a nodal topology format. The nodal topology quantifies the key components of JIE (IAPs, data centers, MPLS fabric, Satellite gateways, DISN Infrastructure Services (DSS) Sites, the optical transport network, Mission Partner Environment Information System w/extension nodes, the Joint Management System for network operations), and a high level alignment (classified / unclassified) to the Cyber Security Reference Architecture (CS RA) and JIE EA. SIPRNET and NIPRNET are the primary computing networks supported by this framework. The JIE Framework puts into perspective the scope of JIE and the relationships of its key components.

Notes:

1. Expeditionary Nodes and Extension Nodes would access VDCs for services
2. Core Data Center (CDC) /Component Enterprise Data Centers (CEDCs) may include on-premises Cloud
3. *Eight JRSS Sites are co-located with CDCs
4. Special Purpose Processing Nodes (SPPNs) are not represented in this SV because of the many variations
5. **CSRA consists of Enterprise Perimeter Protection, Mid-Point, and End-Point Security Appliances and Software. This chart is not meant to provide detailed security locations; but is a general reference to acknowledge the CS defense in depth strategy.**

Acronyms

BAN	Base Area Network	EXP Node	Expeditionary Node	JMS	Joint Management System	On-Prem MS	On-Premise Managed Service
B/P/C/S	Base, Post, Camp, Station	EXT Node	Extension Node	JRSS	Joint Regional Security Stack	REL DMZ	SIPRNet Releasable DMZ
CAP	Cloud Access Point	FED DMZ	SIPRNet Federal DMZ	MPLS	Multi-Protocol Label Switching	SAT GTWY	Satellite Gateway
CDC	Core Enterprise Data Center	GSU	Geographically Separated Unit	NIPR G/W	NIPRNet Federal Gateway	TCN	Tactical Communications Node
CEDC	Component Enterprise Data Center	IAP	Internet Access Point	NOSC	Network Operations/Security Center	TPN	Tactical Processing Node
CMNT	Common Mission Network Transport	IPN	Installation Processing Node	OOB	Out-of-Band Management		
DMCC	DoD Mobile Classified Capability	ISN	Installation Service Node	Off-Prem MS	Off-Premise Managed Service		
DMUC	DoD Mobile Unclassified Capability	JMN	Joint Management Network	OTN	Optical Transport Network		

Data Relationships in CML