DoD Information Enterprise Objective Architecture (IEOA)

13 April 2011

Mr. Walt Okon, Office of DoD CIO/A&I
703-607-0502
walt.okon@osd.mil

Agenda

- DoD Information Enterprise Architecture (IEA) Overview
- Achieving the Purpose of the DoD IEA
- Information Enterprise Objective Architecture (IEOA) Overview
- Enterprise-wide Reference Architecture (RA) Overview

DoD IEA Purpose

- Foster alignment of DoD architectures with the enterprise net-centric vision
- Unify concepts embedded in DoD's net-centric strategies
- Drive common solutions and promote consistency
- Describe the integrated Defense Information Enterprise and the rules for information assets and resources that enable it

DoD Net-Centric Vision

To function as one unified DoD Enterprise, creating an information advantage for our people and mission partners by providing:

- **A rich information sharing environment in which data and services are visible, accessible, understandable, and trusted across the enterprise.**
- **An available and protected network infrastructure (the GIG) that enables responsive information-centric operations using dynamic and interoperable communications and computing capabilities.**

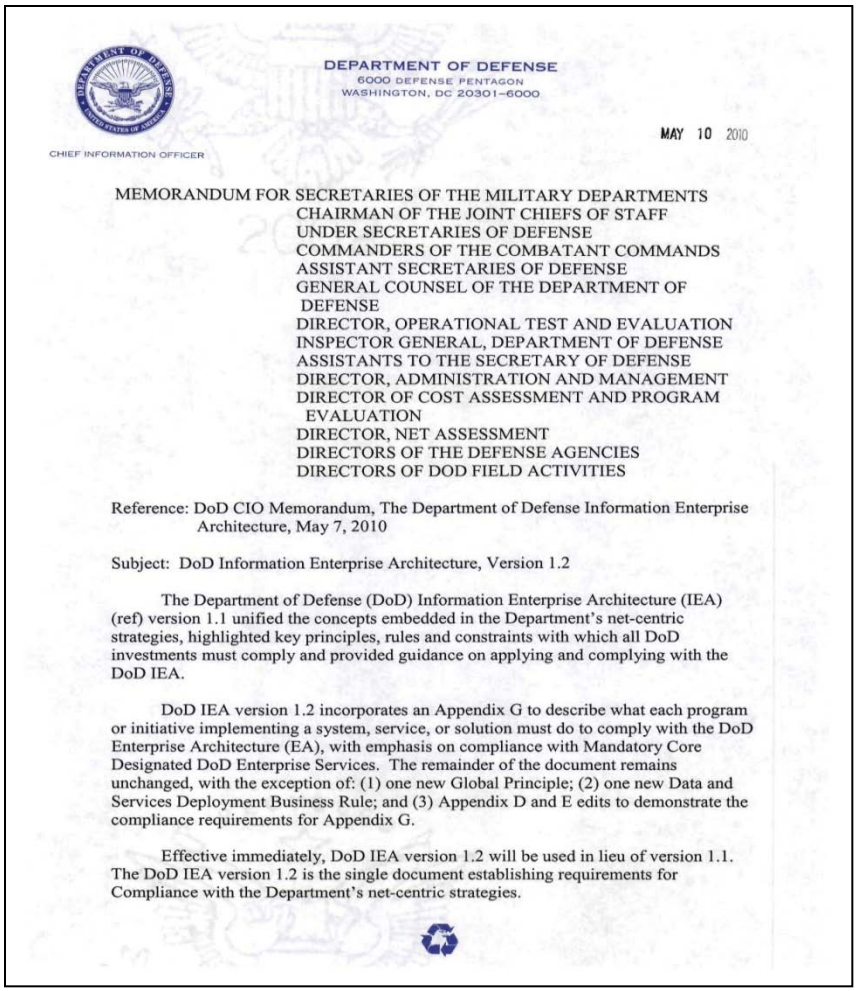
DoD IEA Priority Areas

- **Data and Services Deployment (DSD)** – Decouple data and services from the applications and systems that provide them, allowing them to be visible, accessible, understandable and trusted. Lay the foundation for moving the DoD to a Service-Oriented Architecture (SOA).
- **Secured Availability (SA)** – Ensure data and services are secured and trusted across DoD. Allow users to discover data and services and access them based upon their authorization.
- **Computing Infrastructure Readiness (CIR)** – Provide the necessary computing infrastructure and related services to allow the DoD to dynamically respond to computing needs and to balance loads across the infrastructure.
- **Communications Readiness (CR)** – Ensure that an evolvable transport infrastructure is in place that provides adequate bandwidth and end-to-end, seamless net-centric communications capability across all GIG assets.
- **NetOps Agility (NOA)** – Enable the continuous ability to easily access, manipulate, manage and share any information, from any location at any time.

DoD IEA Priority Areas

- All principles, rules, and activities are grouped by the priority areas
- Priorities were identified as areas where increased attention and investment would drive important progress towards achieving net-centric information sharing
- Priority Areas represent neither organizations nor functions – they are a way to focus efforts across organizations and functional areas to achieve strategic goals

DoD IEA v1.2



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

MAY 10 2010

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR OF COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF DOD FIELD ACTIVITIES

Reference: DoD CIO Memorandum, The Department of Defense Information Enterprise Architecture, May 7, 2010

Subject: DoD Information Enterprise Architecture, Version 1.2

The Department of Defense (DoD) Information Enterprise Architecture (IEA) (ref) version 1.1 unified the concepts embedded in the Department's net-centric strategies, highlighted key principles, rules and constraints with which all DoD investments must comply and provided guidance on applying and complying with the DoD IEA.

DoD IEA version 1.2 incorporates an Appendix G to describe what each program or initiative implementing a system, service, or solution must do to comply with the DoD Enterprise Architecture (EA), with emphasis on compliance with Mandatory Core Designated DoD Enterprise Services. The remainder of the document remains unchanged, with the exception of: (1) one new Global Principle; (2) one new Data and Services Deployment Business Rule; and (3) Appendix D and E edits to demonstrate the compliance requirements for Appendix G.

Effective immediately, DoD IEA version 1.2 will be used in lieu of version 1.1. The DoD IEA version 1.2 is the single document establishing requirements for Compliance with the Department's net-centric strategies.

- Appendix G provides:
  - DoD EA Compliance Requirements
    - DoD IEA
    - Capability & Component EA
    - DISR
    - Compliance with Mandatory Core and Shared Enterprise Services
    - Architecture Registration (DTM 09-013)
  - Table of Mandatory Core and Shared Enterprise Services
- There are no major changes in the primary document.

Achieving the Purpose of the DoD IEA

- The DoD IEA principles, rules, and activities go a long way in achieving the purpose
- More information about the IE is needed to completely fulfill the purpose

Purpose	Status	Solution for Green Status
Foster Architecture Alignment w/Vision		• Describe the concept of operations for the objective IE • Describe the capabilities and services needed to achieve the objective IE • Provide the necessary detail to guide technical direction and IT investment decision-making
Unify Net-Centric Strategies Concepts		
Drive Common Solutions and Consistency		
Describe the Integrated IE; Enabling Rules and Resources		

Need for an Overarching Objective Architecture

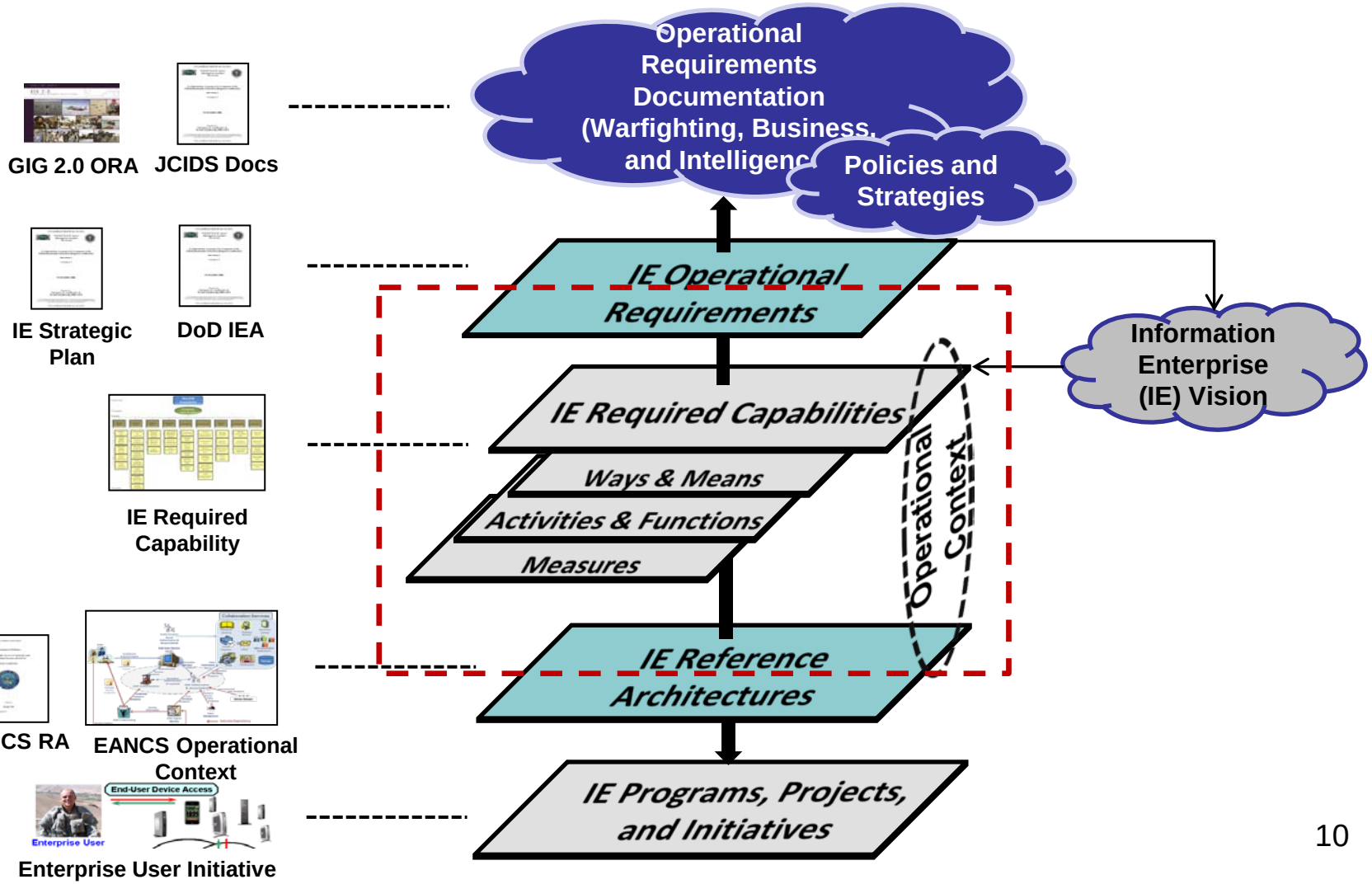
- **Problem**: DoD Senior Leadership has indicated a need for a common picture or description of the DoD Information Enterprise to guide enterprise activities, investments, and solutions to achieve the objective IE vision.
- **An objective DoD IE description must:**
  - Provide a “Big Picture” description of the objective IE
  - Identify and describe in detail the set of required IE capabilities
  - Describe the relationships and dependencies among the capabilities
  - Provide measures for determining progress and success
- **An objective DoD IE description enables:**
  - Identification of needed Enterprise-wide reference architectures
  - Alignment of physical solutions to required IE capabilities
  - Governance and oversight of initiatives, programs, and projects to deliver capabilities
  - Analysis and measurement of progress in achieving the objective IE

An overarching IE Objective Architecture (IEOA) is needed to guide and direct the development of solutions to achieve the objective IE vision

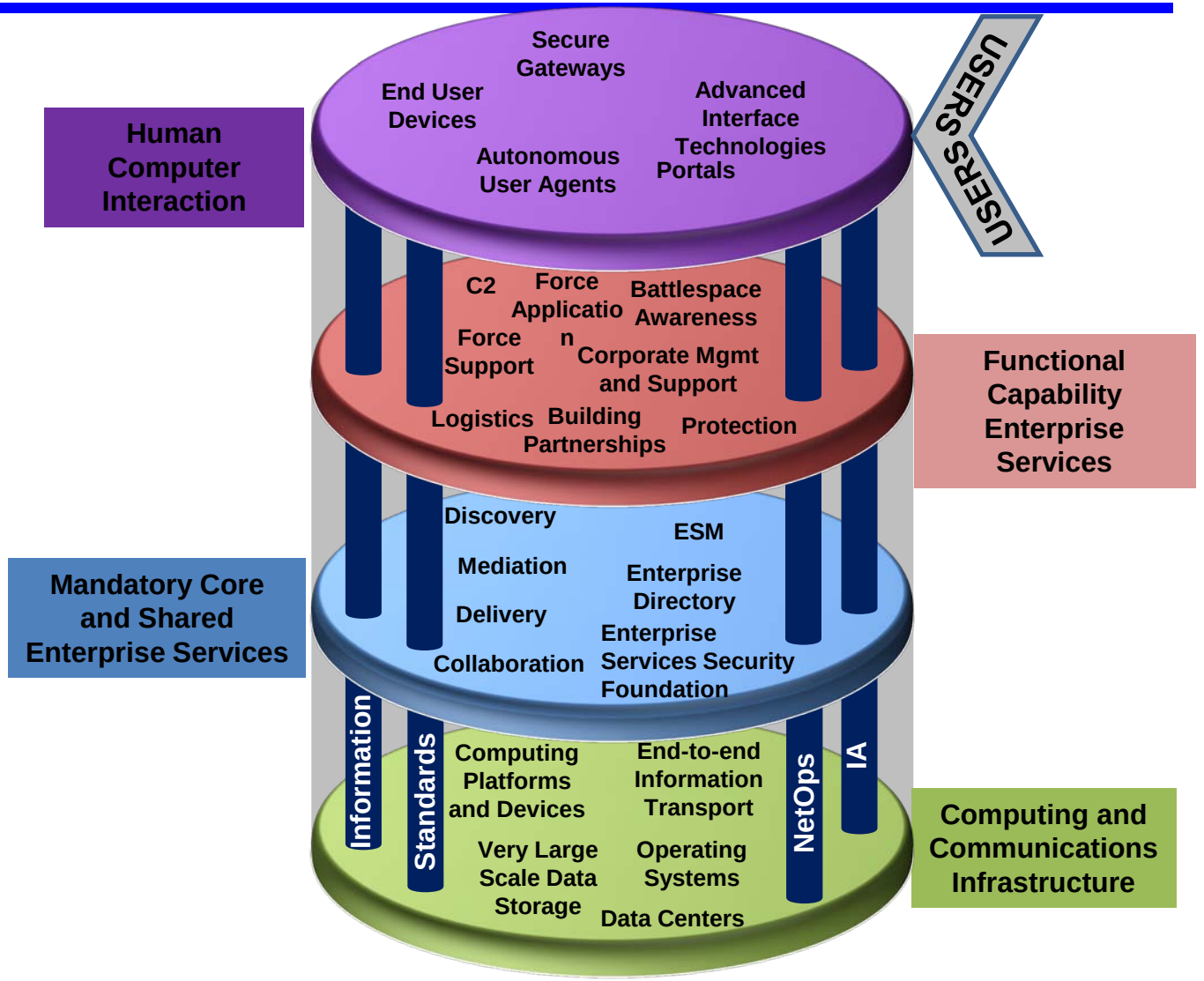
What is the IEOA?

- Architecture description of the objective state for the future Information Enterprise (IE)
- Derived from Operational IT Requirements and IE Strategic Direction
- A key component for establishing **line-of-sight** traceability between strategic objectives and physical solutions
- The IEOA provides :
  - An overarching description of the objective IE; context for all objective IE actions
  - A comprehensive description of the capabilities required in the objective IE (ways and means, activities, functions, and measures)
  - Relationships among IE capabilities
  - The means to identify gaps and evaluate existing initiatives, programs, or projects for providing capabilities
  - The means to identify and direct DoD-wide reference architecture development to guide solutions
  - The means to measure progress toward achieving required IE capabilities

IEOA and the Line-of-Sight Model



Information Enterprise Vision



Notional IEOA Capability Taxonomy (CV-2)

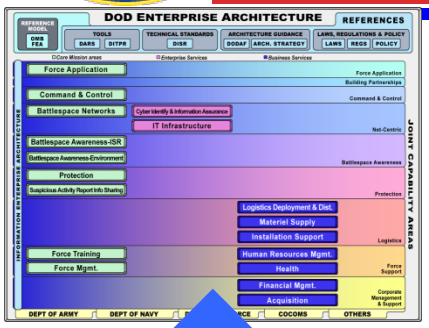
IE Management and Oversight	IE Protection and Security	IE Control and Operation	IE Infrastructure
Common, enforceable policies and standards	Threat Assessment of IE Operations	Automated Configuration Changes	Information Transport
Standard Protocols for Information Transmittal and Acknowledgement	IE Incident Response	Dynamic Configuration Prioritization and Alignment	Guaranteed Global Connectivity
Governance/Oversight of IE Development/ Implementation	Data and Metadata Protection	Dynamic Policy-based Management and Routing	Continuity of operations and disaster recovery
Architecture Development and Use	Portable Identity Credential Provision and Management	Integrated Network Operations	Infrastructure as One Virtual Capability
Authoritative Body Identification and Empowerment	Cross Security Domain Information Exchange	Flexible, Dynamic Non-interfering Spectrum Use	Data and Service Discovery and Availability

Intended Use for the IEOA

- Guide DoD actions in achieving the IE objective state
- Inform assessment and evaluation of IE related architecture
- **Identify potential areas for reference architecture (RA) development**
- Guide IT technical direction through capabilities and services descriptions and Enterprise-wide Reference Architecture (RA)
- Inform DoD IT investment decision-making

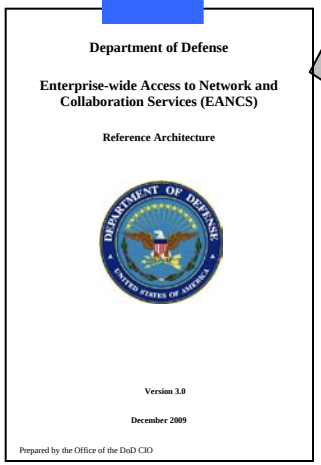
DoD-wide Reference Architecture

Architecture Artifacts



Architecture Federation

RA Document



Department of Defense

Enterprise-wide Access to Network and Collaboration Services (EANCS)

Reference Architecture

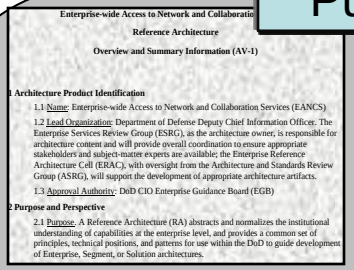
Version 3.0

December 2009

Prepared by the Office of the DoD CIO

Provides Department-level guidance in the form of context, rules, patterns, and technical positions

Strategic Purpose



Enterprise-wide Access to Network and Collaboration Services (EANCS)

Reference Architecture

Overview and Summary Information (AV-1)

1 Architecture Product Identification

1.1 Name: Enterprise-wide Access to Network and Collaboration Services (EANCS)

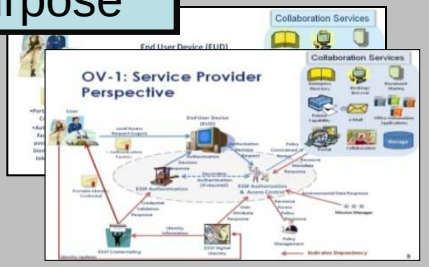
1.2 Lead Organization: Department of Defense Deputy Chief Information Officer. The Enterprise Services Review Group (ESRG), as the architecture owner, is responsible for architecture content and will provide overall coordination to ensure appropriate stakeholders and subject-matter experts are available; the Enterprise Reference Architecture Cell (ERAC), with oversight from the Architecture and Standards Review Group (ASRG), will support the development of appropriate architecture artifacts.

1.3 Approval Authority: DoD CIO Enterprise Guidance Board (EGB)

2 Purpose and Perspective

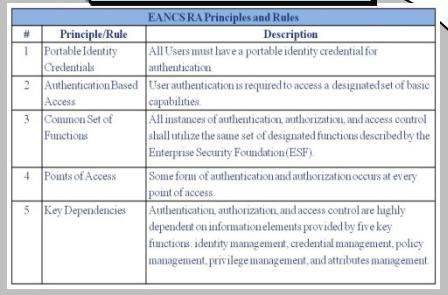
2.1 Purpose. A Reference Architecture (RA) abstracts and normalizes the institutional understanding of capabilities at the enterprise level, and provides a common set of principles, technical positions, and patterns for use within the DoD to guide development of Enterprise, Segment, or Solution architectures.

AV-1 (Overview and Summary)



OV-1 (Concept – Consumer & Provider)

Principles

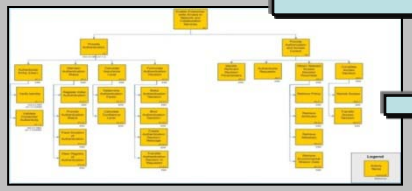


EANCS RA Principles and Rules

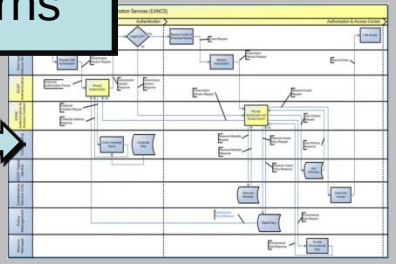
#	Principle/Rule	Description
1	Portable Identity Credentials	All Users must have a portable identity credential for authentication.
2	Authentication Based Access	User authentication is required to access a designated set of basic capabilities.
3	Common Set of Functions	All instances of authentication, authorization, and access control shall utilize the same set of designated functions described by the Enterprise Security Foundation (ESF).
4	Points of Access	Some form of authentication and authorization occurs at every point of access.
5	Key Dependencies	Authentication, authorization, and access control are highly dependent on information elements provided by five key functions: identity management, credential management, policy management, privilege management, and attributes management.

OV-6a (Operational Rules Model)

Patterns

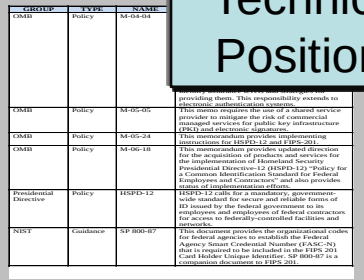


OV-5a (Activity Decomposition)



OV-6c (Event-Trace Description)

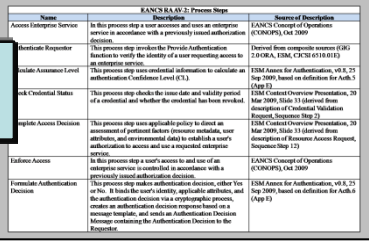
Technical Positions



GROUP	TYPE	NAME	
OMB	Policy	M-04-04	providing them. This responsibility extends to electronic authentication systems.
OMB	Policy	M-05-05	This memorandum designates a shared service provider to mitigate the risk of commercial managed services for public key infrastructure (PKI) and electronic signatures.
OMB	Policy	M-05-24	This memorandum provides implementing instructions for HSPD-12 and FIPS-201.
OMB	Policy	M-06-18	This memorandum provides updated direction for the acquisition of products and services for the implementation of Homeland Security Presidential Directive-12 (HSPD-12) "Policy for a Common Identification Standard for Federal Employees and Contractors" and also provides status of implementation efforts.
Presidential Directive	Policy	HSPD-12	HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of ID issued by the federal government to its employees and employees of federal contractors for access to federally-controlled facilities and networks.
NIST	Guidance	SP 800-87	This document provides the organizational codes for federal agencies to establish the Federal Agency Smart Credential Number (FASC-N) and Agency Code portions of the Federal Agency Card Holder Unique Identifier. SP 800-87 is a companion document to FIPS 201.

StdV-1 (Standards Profile)

Vocabulary



EANCS RA AV-2: Process Steps

Name	Description	Source of Description
Access Enterprise Service	In this process step a user accesses and uses an enterprise service in accordance with a previously issued authorization decision.	EANCS Concept of Operations (CONOPS), Oct 2009
Authenticate Requestor	This process step invokes the Provide Authentication function to verify the identity of a user requesting access to an enterprise service.	Derived from composite sources (GIG 2.0 ORA, ESM, CICSI 6510.01E)
Calculate Assurance Level	This process step uses credential information to calculate an authentication Confidence Level (CL).	ESM Annex for Authentication, v0.8, 25 Sep 2009, based on definition for Auth.5 (App E)
Check Credential Status	This process step checks the issue date and validity period of a credential and whether the credential has been revoked.	ESM Context Overview Presentation, 20 Mar 2009, Slide 33 (derived from description of Credential Validation Request, Sequence Step 2)
Complete Access Decision	This process step uses applicable policy to direct an assessment of pertinent factors (resource metadata, user attributes, and environmental data) to establish a user's authorization to access and use a requested enterprise service.	ESM Context Overview Presentation, 20 Mar 2009, Slide 33 (derived from description of Resource Access Request, Sequence Step 12)
Enforce Access	In this process step a user's access to and use of an enterprise service is controlled in accordance with a previously issued authorization decision.	EANCS Concept of Operations (CONOPS), Oct 2009
Formulate Authentication Decision	This process step makes authentication decision, either Yes or No. It binds the user's identity, applicable attributes, and the authentication decision via a cryptographic process, creates an authentication decision response based on a message template, and sends an Authentication Decision Message containing the Authentication Decision to the Requestor.	ESM Annex for Authentication, v0.8, 25 Sep 2009, based on definition for Auth.6 (App E)

AV-2 (Integrated Dictionary)

Backup Slides

Examples of DoD IEA Rules

- **Data and Services Deployment (DSD)**: **DSDR 01** - Authoritative data assets, services, and applications shall be accessible to all authorized users in the Department of Defense, and accessible except where limited by law, policy, security classification, or operational necessity.
- **Secured Availability (SA)**: **SAR 08** - Metadata containing access control and quality of protection attributes shall be strongly bound to or associated with information assets and utilized for access decisions.
- **Computing Infrastructure Readiness (CIR)**: **CIR 01** - Computing infrastructure shall be consolidated, to the greatest extent possible, so that fixed global/regional and deployed virtual CI resources are used efficiently.
- **Communications Readiness (CR)**: **CRR 03** - GIG communications systems shall be acquired to support migration to a Cipher Text (CT) core. CT networks and segments shall transport both classified and unclassified encrypted traffic.
- **NetOps Agility (NOA)**: **NOAR 01** - The DoD must continue to transform the NetOps C2 into a unified and agile construct with centralized direction and decentralized execution to effectively respond to unanticipated situations on the time scale of cyber attack.

IEOA: Summary of Capabilities

- **Manage and Oversee the IE**: Common, enforceable policies and standards for the IE; standard protocols for information exchanges; standard security engineering processes; use of best practices from government, industry, and academia; governance structures and processes for developing and implementing the IE; development and use of architectures; authoritative bodies to govern information sharing; sharing of service expenses; and implementation of National Green IT initiatives.

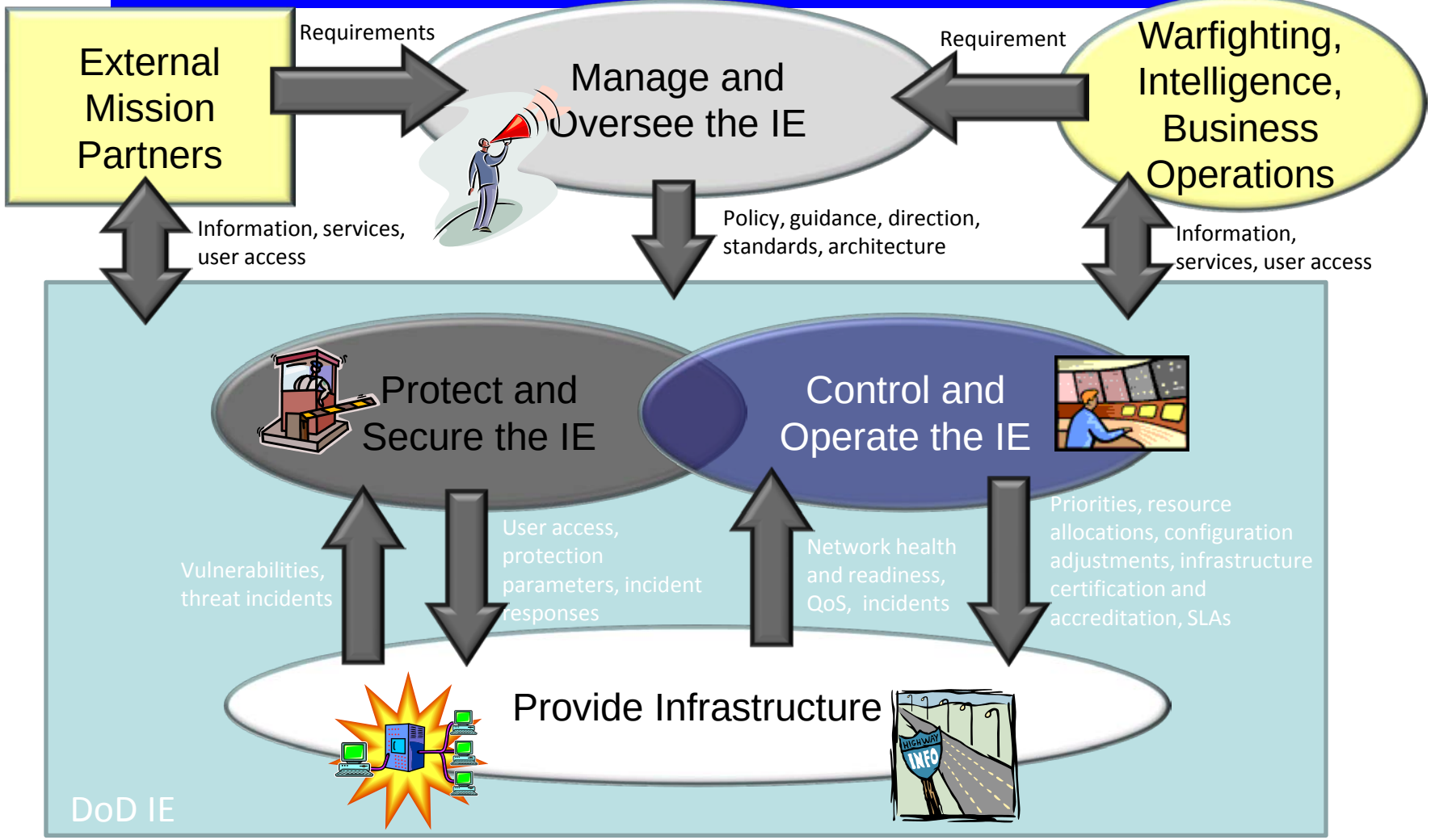
- **Protect and Secure the IE**: Threat and risk analysis of the IT supply chain; vulnerability analysis; rapid and secure response to threats and attacks; network defense in depth; protection of data and metadata at rest, during processing, and in transit; assured access to information and services; digital identities; portable identity credentials; monitoring of sensitive/classified information; and cross security domain information exchange.

IEOA: Summary of Capabilities

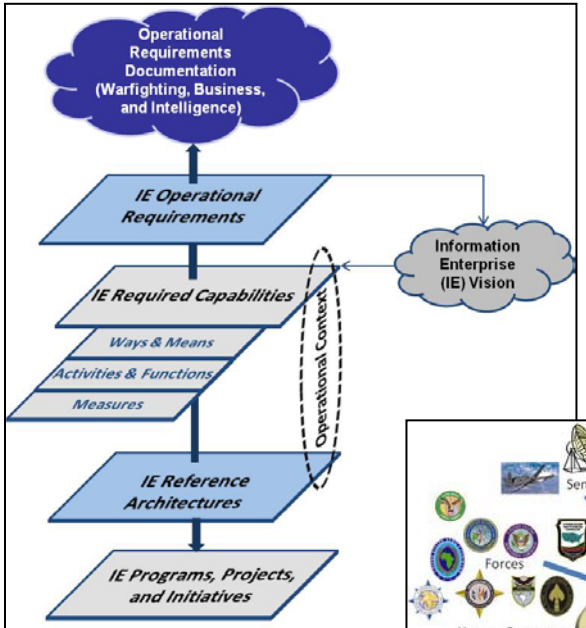
- **Control and Operate the IE**: Automated configuration updates; prioritization and dynamic adjustment of IE resources; deployment and installation of adhoc networks; dynamic routing and policy-based management systems; infrastructure accreditation, certification, and approval; network situational awareness; health and mission readiness metrics; information dissemination priorities; service level monitoring and controls; flexible and dynamic electromagnetic spectrum management; standardized education and training of users/operators; and integrated network operations.

- **Provide Infrastructure**: Information transport for end-to-end communications; voice, video, and data traffic on a single network; global connectivity to the network; operational bandwidth assessment for new services; globally open, stable, and secure Internet for collaboration; continuity of operations and disaster recovery; virtual infrastructure; interoperability with components and mission partners; identification, evaluation, test, and employment of new technologies; digital user and service attributes; digital policy management and use; NetOps-enabled resources; authoritative data and capabilities offered as services; knowledge sharing; real-time collaboration tools; foreign language processing; processing, integration, and fusion of multi-source data; information sharing with coalition and external mission partners; and data, services, and information available and discoverable across the IE.

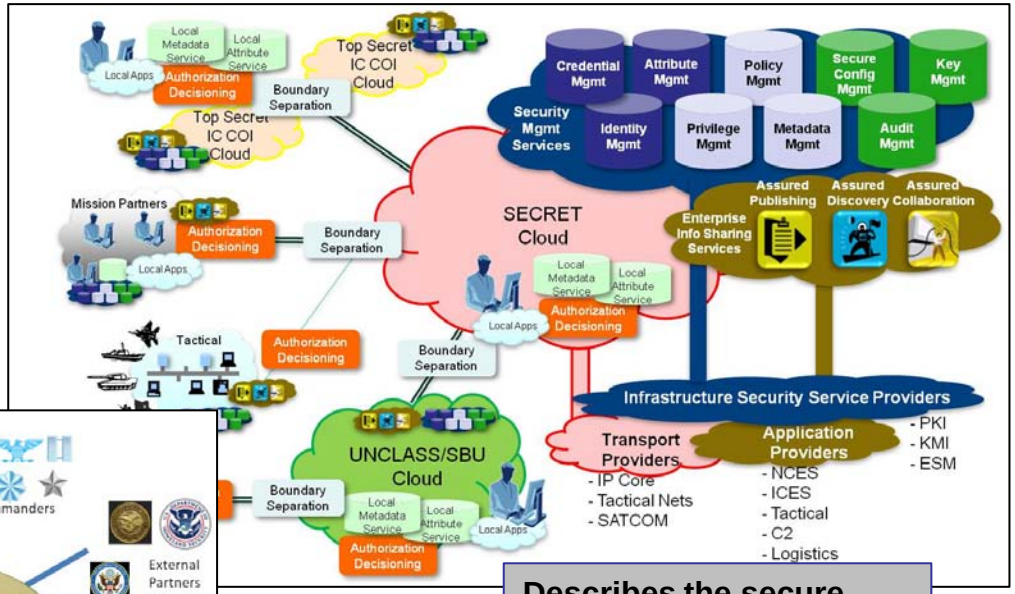
IEOA High-level Operational Concept Graphic (OV-1)



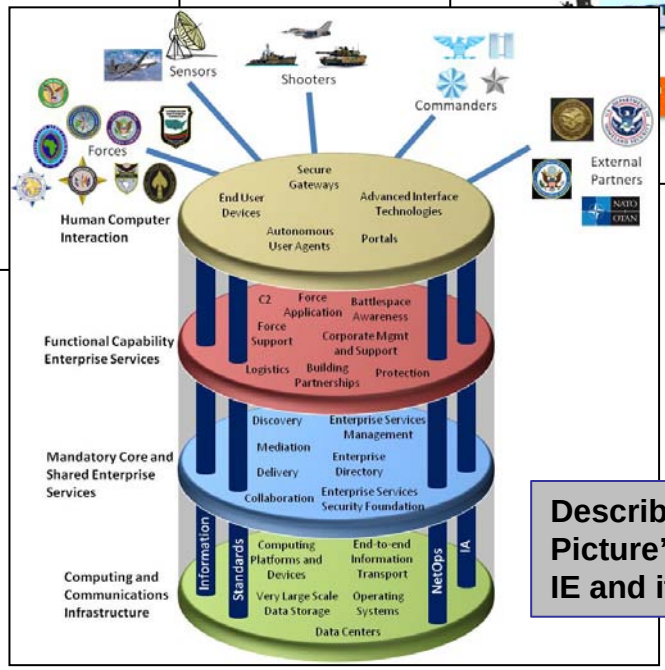
IEOA: Sample Descriptions



Describes the Line-of-Sight from operational requirements to physical Solutions.



Describes the secure environment necessary for effective, assured information sharing.



Describes the "Big Picture" of the objective IE and its parts.