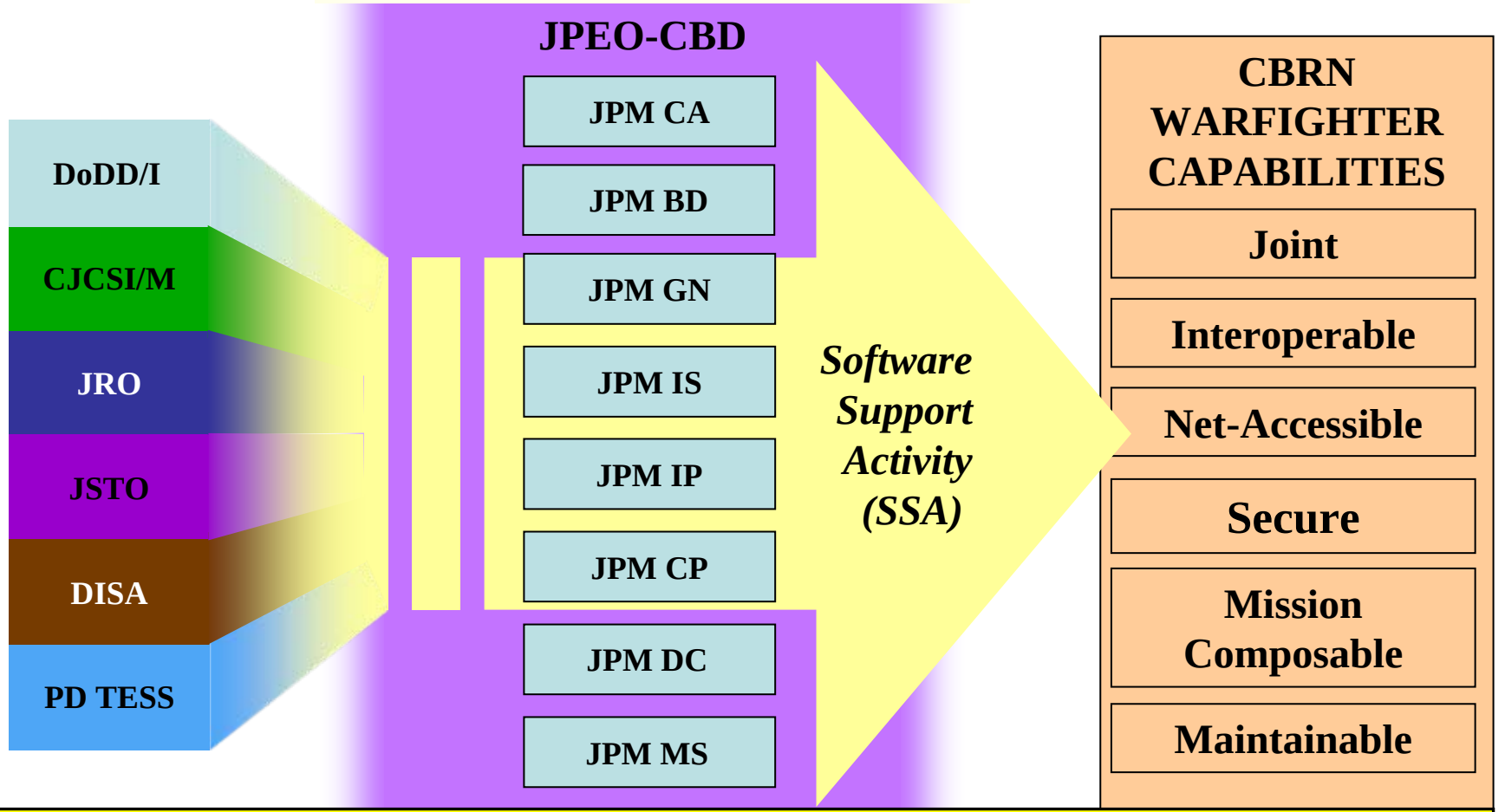
JPEO CBD
Software Support Activity
(Net-Centric Services)
January 9, 2007

Kevin Adams
Chief, Future Technologies
SSA Director
kevin.adams@jpmis.mil

Agenda

1. SSA Overview
2. GIG and Net-Centric Issues
   - C2 Transition to SOA
   - Migration Strategy
3. How Do We Meet the Challenge
4. Leveraging Activities
5. Road Ahead

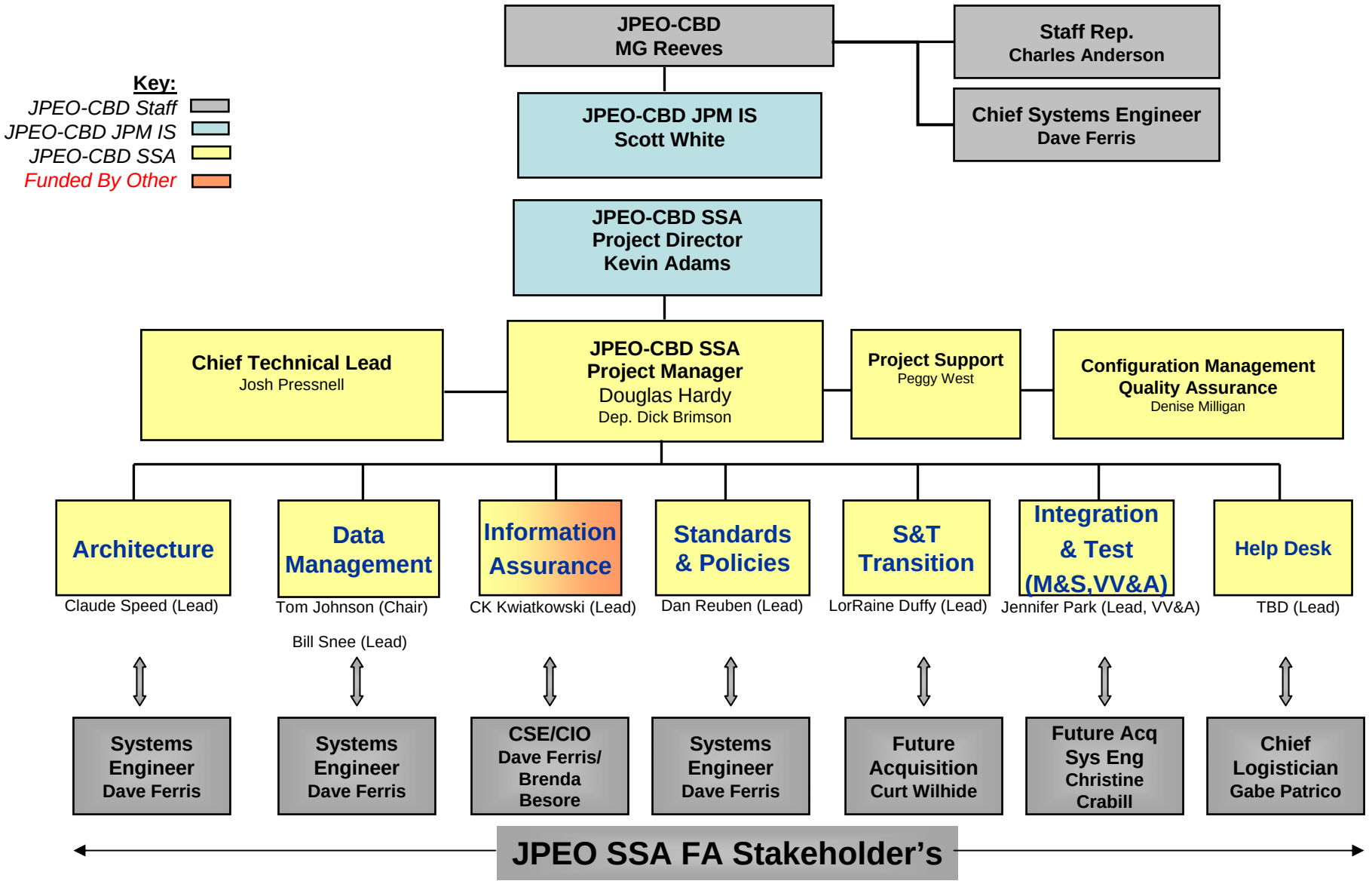
CBRN-SSA Vision



SSA WORKS TO REALIZE THE VISION OF NET-CENTRIC WARFARE -

Cost effective single point of contact for users (Customers, Developers, and Warfighters) to receive professional and timely assistance with all CBRN Defense program standards, interoperability, and supportability needs to ultimately facilitate the creation of more efficient, common, and consistently superior *interoperable and integrated* CBRN systems.

SSA FY07 Organization



GIG Compliance

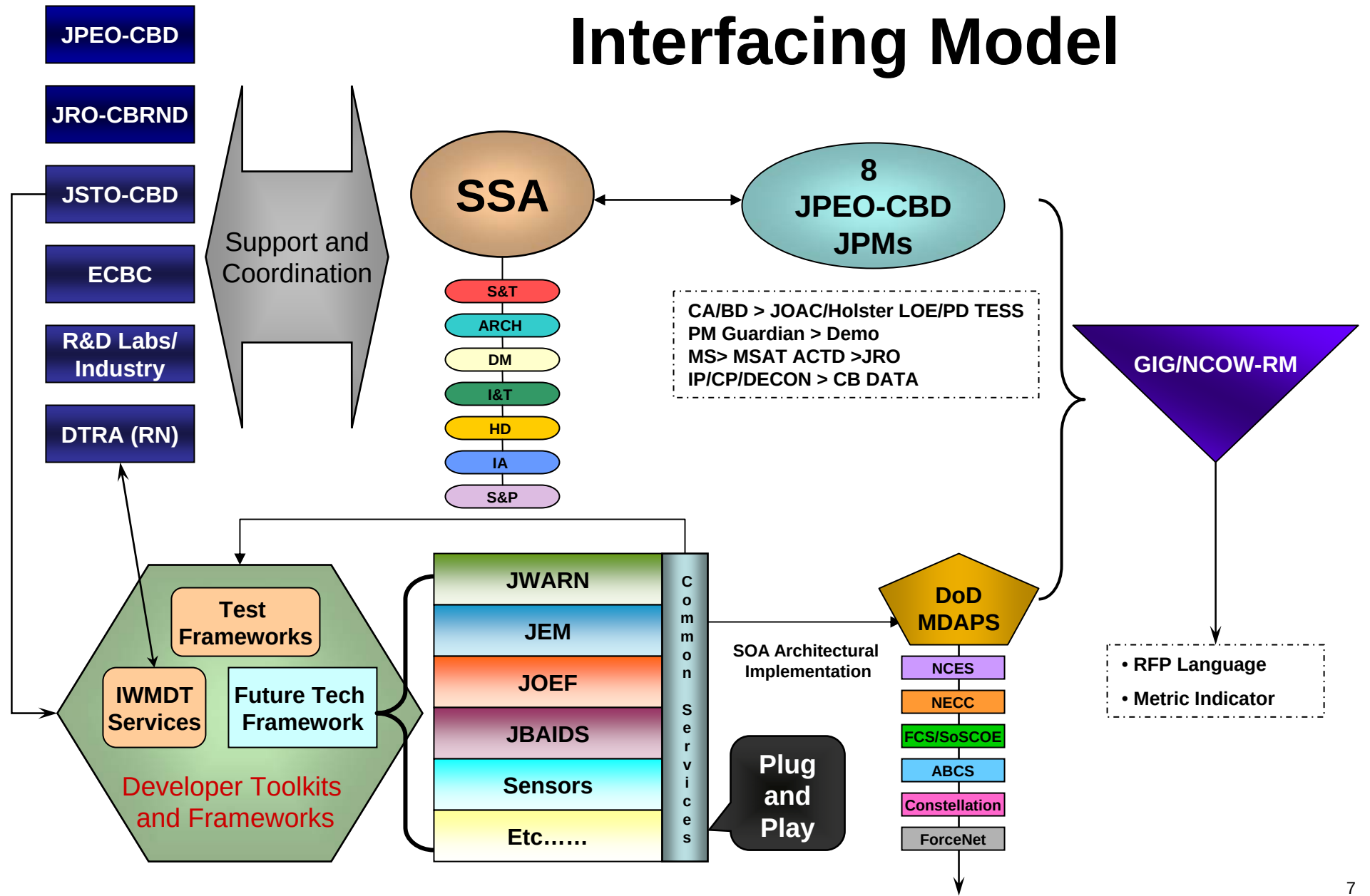
- Compliance with the GIG means an information technology-based initiative or an acquisition program, throughout its lifecycle:
- Meets the DoD Architecture Framework (DoDAF) requirements.
- Meets the Core Architecture Data Model (CADM) requirements for using/reusing architecture data.
- Meets the DoD Information Technology Standards Registry (DISR) requirements in selecting technologies and standards.
- Meets the DoD Net-Centric Data Strategy requirements and intent.
- Explicitly addresses net-centricity and determine the program's net-centric correspondence to key net-centric criteria (e.g., concepts, processes, services, technologies, standards, and taxonomy). (For further information see the Net-Centric Operations and Warfare Reference Model (NCOW RM) Compliance Assessment Methodology (Draft) - found on the GIG Architecture website).
- Meets the broad requirements set forth in the GIG Capstone Requirements Document.

*NCOW RM

- The NCOW RM is focused on achieving net-centricity. Compliance with the NCOW RM translates to articulating how each program approaches and implements net-centric features. Compliance does not require separate documentation; rather, it requires that program managers and Sponsors/Domain Owners address, within existing architecture, analysis, and program architecture documentation, the issues identified by using the model, and further, that they make explicit the path to net-centricity the program is taking.

*Net-Centric Operational Warfare Reference Model

Net-Centric Interfacing Model



Net-Centricity – What We Need to Know

- **Each of the Services are migrating to SOA**
  - **ForceNet, FCS/SoSCOE, and Army Enterprise Architecture (AEA), Constellation NECC/NCES**
- **Enterprise Services are being defined**
  - **Data**
  - **Security**
  - **User interfacing standardization**
- **CBRN capabilities need to be modular and plug into various networks easily**
  - **Plug and Play**
  - **Composeable**
  - **Scalable**
- **MDAP will drive the Architecture**
  - **C2 Systems will have open Architecture and Standards**

MDAP Integration

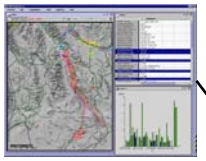
Will require expertise and understanding of the following:

- Systems and Software Analysis, Architecture, Engineering, and Evaluation
- Networking of Sensors and Systems
- Distributed Web-Based Sensors
- Net-centric computing and network algorithms
- CBRN Sensor Emulation
- C4ISR / C2
- Data Modeling (CBRN Data Model and XML Schema)
- Service Oriented Architectures
- Expert Systems, Intelligent Agents, Distributed and Parallel Computing
- Embedded systems
- Real-Time Systems
- Networked Communications (wireless and wired)
- Modeling and Simulation (Expertise, Tools, Technology, Frameworks, Standards)
- Information Assurance Planning, Strategies, Process, Policy and Execution, and System Security Accreditations
- Standards and Interfaces for Models, Information Systems, and Sensors

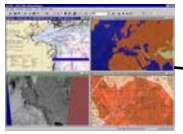
How Do We Meet the Challenge?

Joint Integrated Modular Mission Configurable Networked CBRN Capabilities

CBRN-Enabled GIG via CBRN IS



Networked CBRN Net-Centric COPs enabled by JPM Information Systems, NCES and NECC…



CBRN Warning, Reporting, Alerting, Plans, Course of Action, CBRN Status and Readiness

01 10 01 10 01 10 01 10 01 10 01 10 01 10 01 10 01 10 01 10 01 10 01 10 01 10 01 10 01 10

GIG

HHQ / Strategic

Installations

Afloat (DDX)

Tactical Units (FCS)

Warfighter

CBRN Sensing

Fixed, mobile, and platform embedded Integrated sensing capabilities

Integrated Warning and Reporting, Hazard Prediction, Course of Action, and Consequence Management

Pervasive CBRN Networked Intel

CBRN Medical Treatment

Prophylaxis and triage

Remove the threat, preserve the Warfighter and the Equipment

Individual Protection

Continued CBRN-Protected Individual Mission Execution

Integrated Protection for Installations, Units, and Vehicles on the move

CBRN Defense Capabilities Required at all Echelons and on all Platforms for Mission Effectiveness!

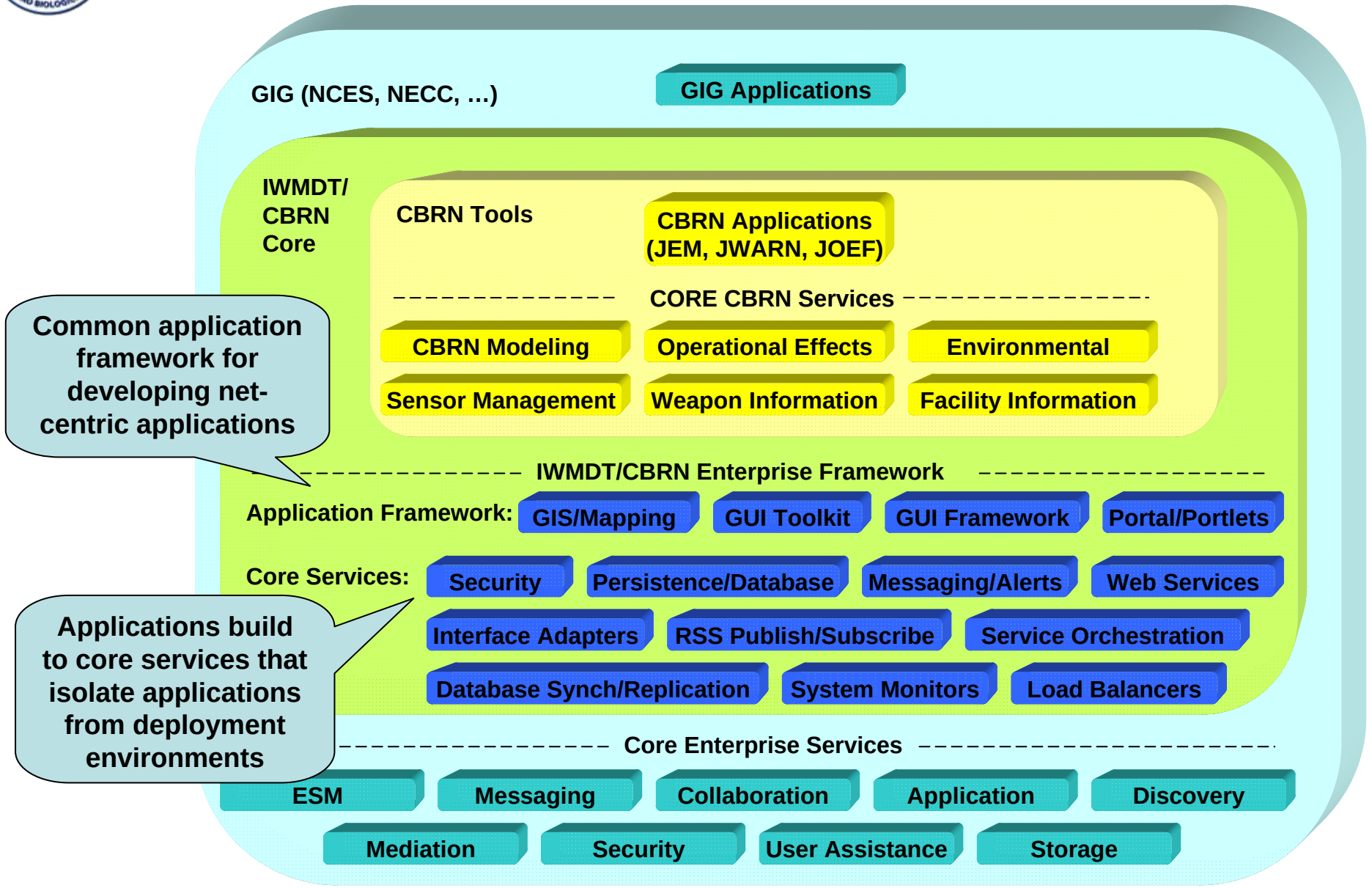
CBRN Data Model Supports Net-Centric Data Strategy

- Enables the grouping of services to create a system of systems
- Defines common data elements when creating a web service
- Used to make CBRN data discoverable and accessible
- Eliminates point-to-point interface development
- Used to Create the CBRN XML Schema
- Reusable data definitions
- Shortens System Development Time
- Facilitates Reuse of System Components
- Allows for investment in component improvement versus component reinvention
- Requires sustainment under POR purview

Current S&T Efforts Supporting Common Services

- JSTO Sponsored Shared Common Operating Picture (COP) for HLS and HLD
  - Integrated shared COP capabilities for HLS/HLD
    - Mostly message integration
    - JEM proxy
  - Currently in phase 2
- JSTO Sponsored Common CBRN Software Services
  - A common framework to support Net-Centric Components and Services environments.
    - NCES, NECC, SoSCOE, ForceNet e.g.
- NECC & NCES pilots
  - Awaiting Approval
- Program risk reduction pilots and LOEs
  - JCID on a Chip (JoaC)
  - COE decoupling pilots
  - Technical decision pilots
  - Holster LOE (JPEO-CBD initiative)

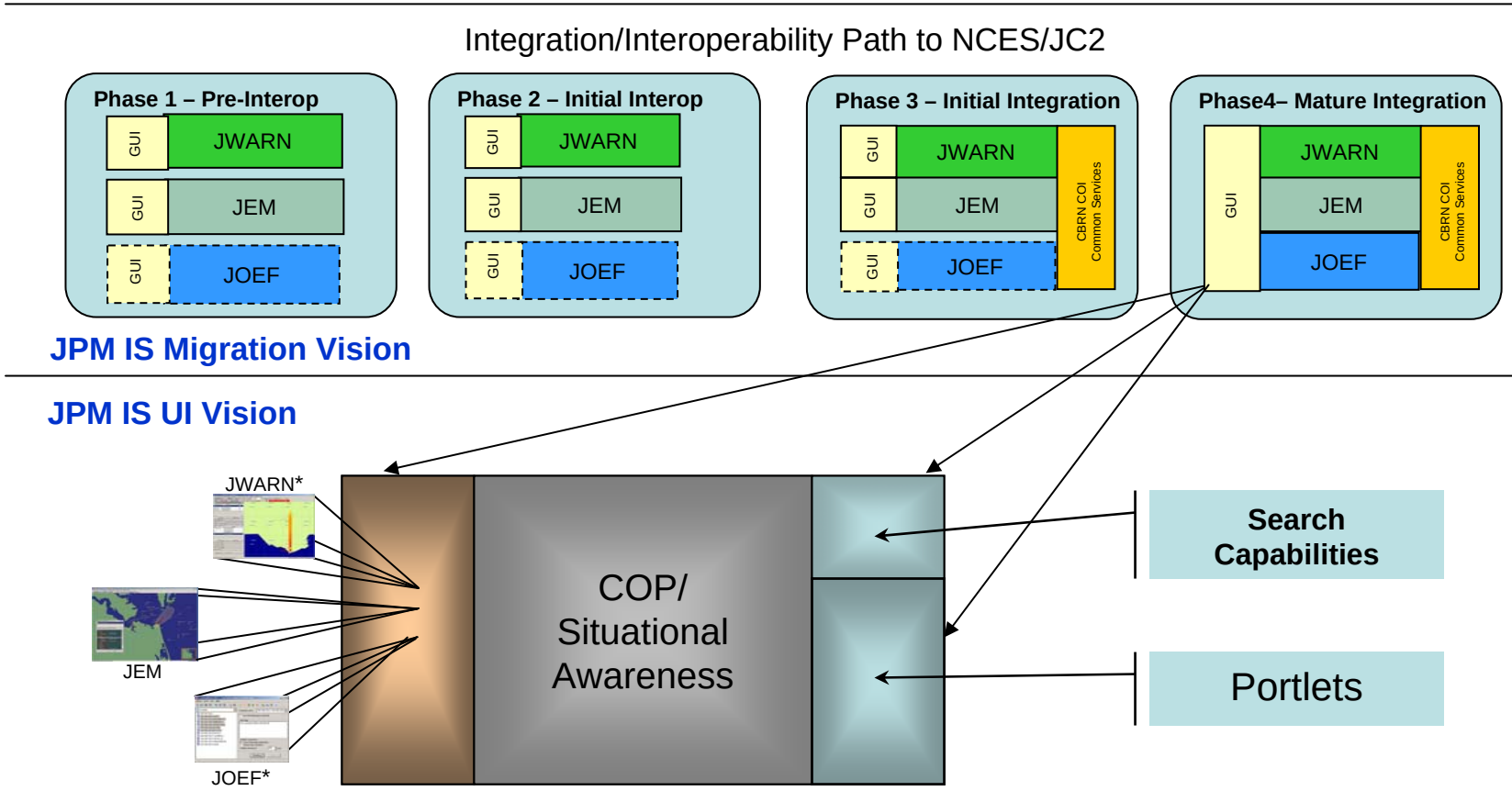
Proposed Leveraging Activities - Tech Base Architecture



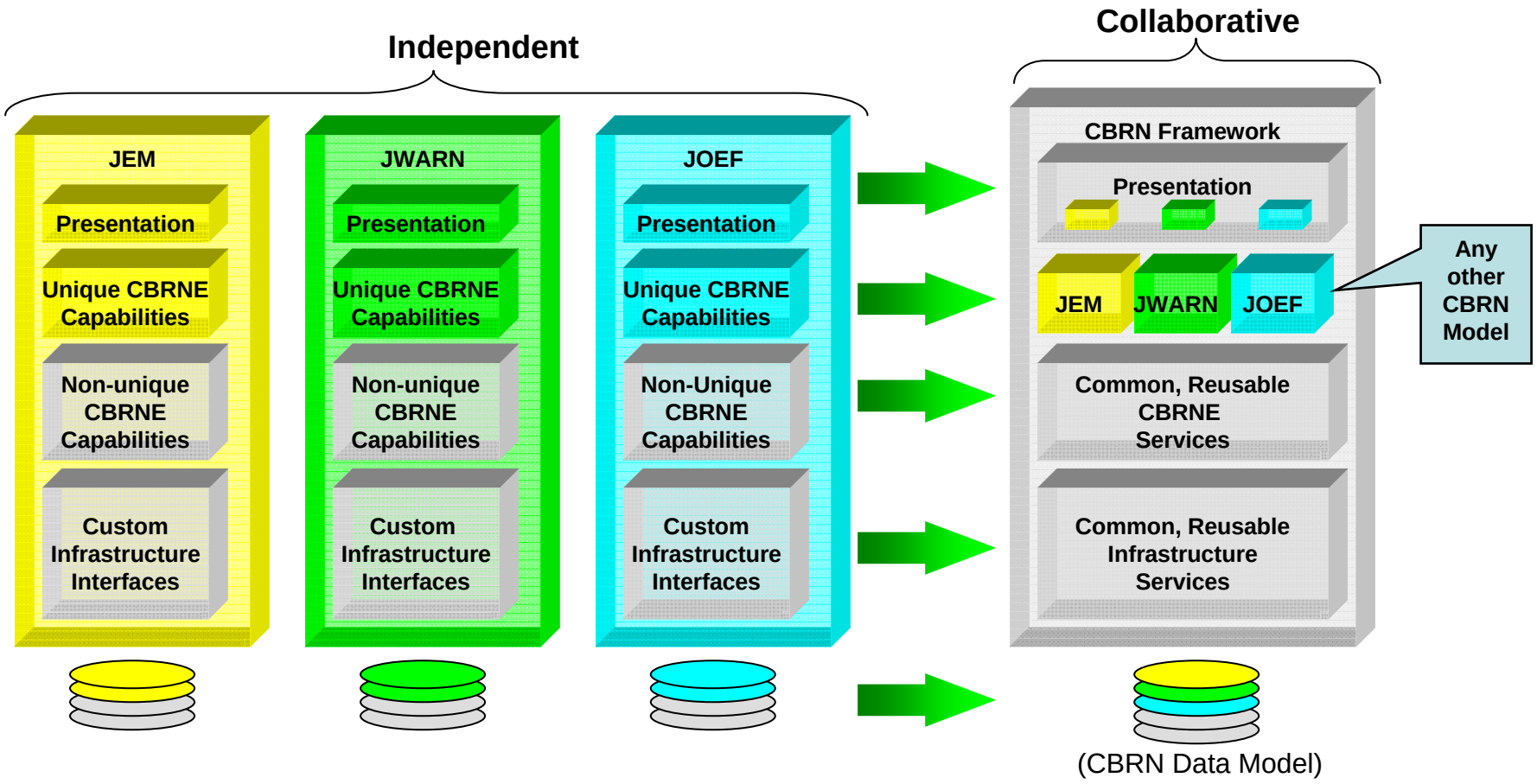
Leveraging JPM IS Integrated Product Vision

Provide CBRN products in a timely and efficient manner to the warfighter and first responder

- **Integrated family of products**
- **Single integrated user interface to all services**



Maximize Re-Use at all Levels



Road Ahead for a Common CBRN Framework

- **Review Message Sharing Requirements**
  - **Mediation service for Message conversion**
  - **Architecture for message converters and parsers**
- **Implement a Common GIS Framework**
  - **Same code base to; WebCOP, C2PC, Googlemaps, JWC.**
- **Put in Place an Open Architecture Approach to Integration**
  - **Allows decoupled messaging**
  - **Middleware agnostic**
  - **Insulation of program development cycles from others**
- **Open Architecture approach for Sensor Integration**
  - **Common front end to JWARN to allow multiple sensor networks**
- **Support Common Net-Centric Services**

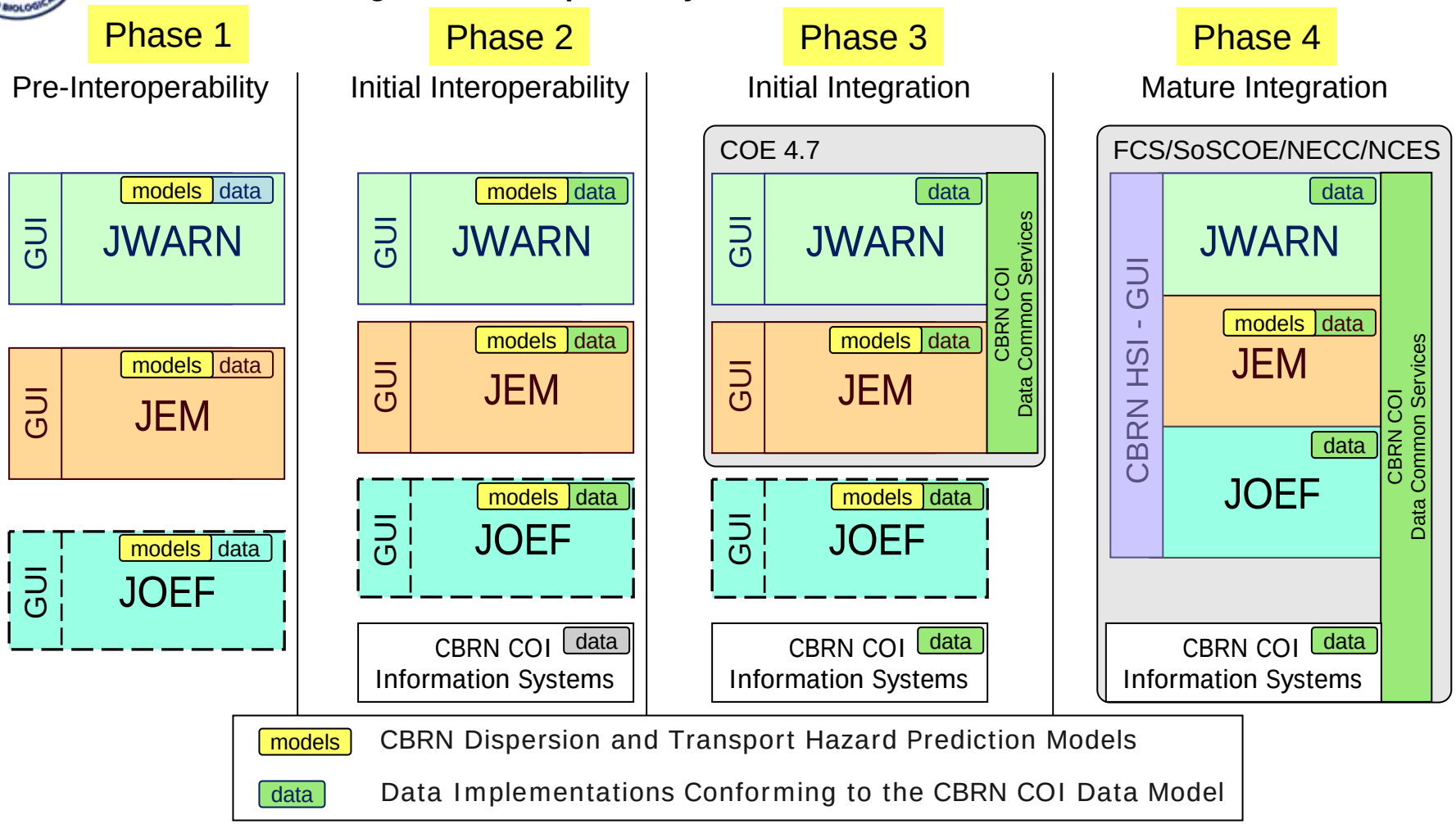
SSA Goals

- **Need to reduce lifecycle cost of JPEO-CBD products and artifacts as they relate to MDAP integration and interoperability.**
- **Increase collaboration and coordination in the CBRN development community.**
- **Maximize flexibility, reuse, and portability of software components.**
- **Reduce interfacing (outward looking) software for each POR.**
- **Align Tech Base under a SOA to transition to the user/warfighter product faster and cheaper.**

Impacts SENSE/SHAPE/SHIELD/SUSTAIN

BACKUPS

JPM IS Migration Strategy
Integration/Interoperability Path to FCS/NCES/NECC/Etc.

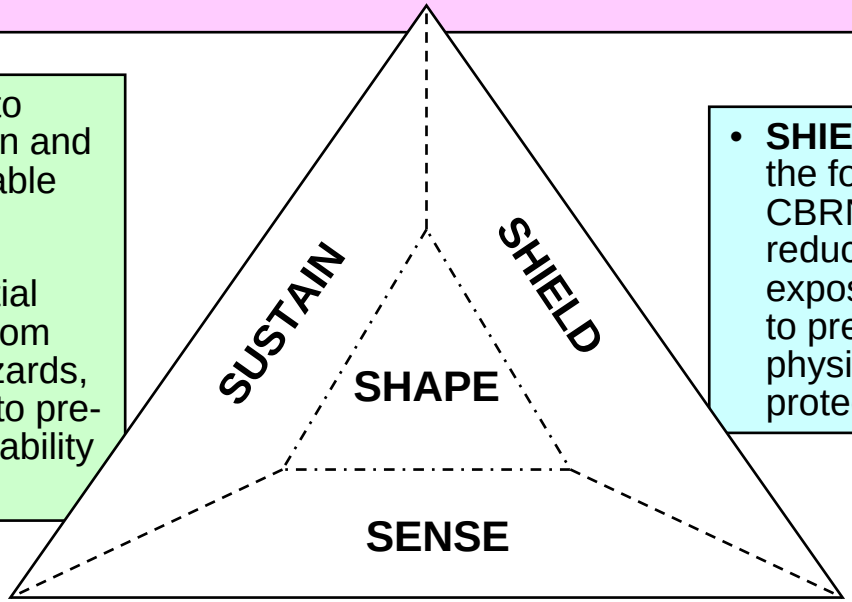


ARCHITECTURE MIGRATION STRATEGY - *DISCIPLINED EVOLUTION OF DESIGN TO MEET THE VISION!*

Joint CBRN Defense Functional Concept

- **SHAPE –** Provides the ability to characterize the CBRN hazard to the force commander - develop a clear understanding of the current and predicted CBRN situation; collect and assimilate info from sensors, intelligence, medical, etc., in near real time to inform personnel, provide actual and potential impacts of CBRN hazards; envision critical SENSE, SHIELD and SUSTAIN end states (preparation for operations); visualize the sequence of events that moves the force from its current state to those end states.

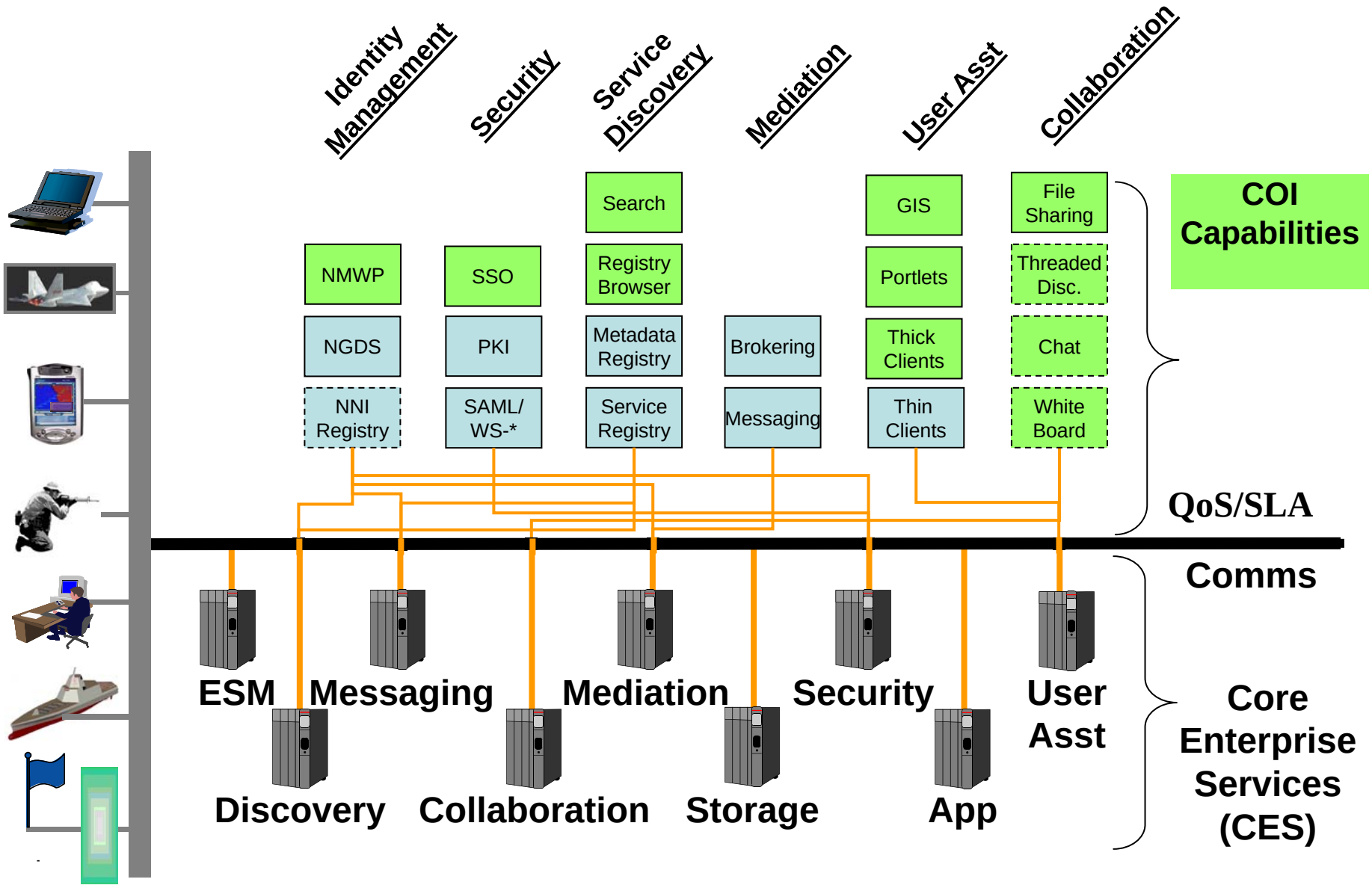
- **SUSTAIN –** The ability to conduct decontamination and medical actions that enable the quick restoration of combat power, maintain/recover essential functions that are free from the effects of CBRN hazards, and facilitate the return to pre-incident operational capability as soon as possible.



- **SHIELD –**The capability to shield the force from harm caused by CBRN hazards by preventing or reducing individual and collective exposures, applying prophylaxis to prevent or mitigate negative physiological effects, and protecting critical equipment

- **SENSE – The capability to continually provide the information about the CBRN situation at a time and place by detecting, identifying, and quantifying CBRN hazards in air, water, on land, on personnel, equipment or facilities. This capability includes detecting, identifying, and quantifying those CBRN hazards in all physical states (solid, liquid, gas).**

TO - BE


Identity Management
Security
Service Discovery
Mediation
User Asst
Collaboration
NMWP
NGDS
NNI Registry
SSO
PKI
SAML/ WS-*
Search
Registry Browser
Metadata Registry
Service Registry
Brokering
Messaging
GIS
Portlets
Thick Clients
Thin Clients
File Sharing
Threaded Disc.
Chat
White Board
COI Capabilities
QoS/SLA
Comms
ESM
Messaging
Mediation
Security
User Asst
Discovery
Collaboration
Storage
App
Core Enterprise Services (CES)

DoD Current Activities

- GIS interoperability
  - GIS applications availability via common open standards (OGC)
    - GIS targets
      - FalconView, Joint WebCOP(JWC), OSWebCOP, Joint Battlespace Viewer (JBV), googleMap, GoogleEarth, C2PC
- COE migration to SOA's
  - Messaging
    - Using Exchange and outlook plugins from DMS program to bridge from COE to COTS
    - Migrate off CMP and UCP
  - Publish/Subscribe
    - Leveraging current GCCS-M initiatives like Joint translator forwarder(JXF).
    - Asynchronous messaging using JMS and the BEAWLS segments
    - RT Bridges - NDDS, OMG-DDS, SPLICE
  - Registry/directory for lookups
    - Active Directory to LDAP configurations for finding services and enterprise management of users and applications
    - NCES Service discovery and Service Registry (UDDI)

IWMDT Software Architecture Layers