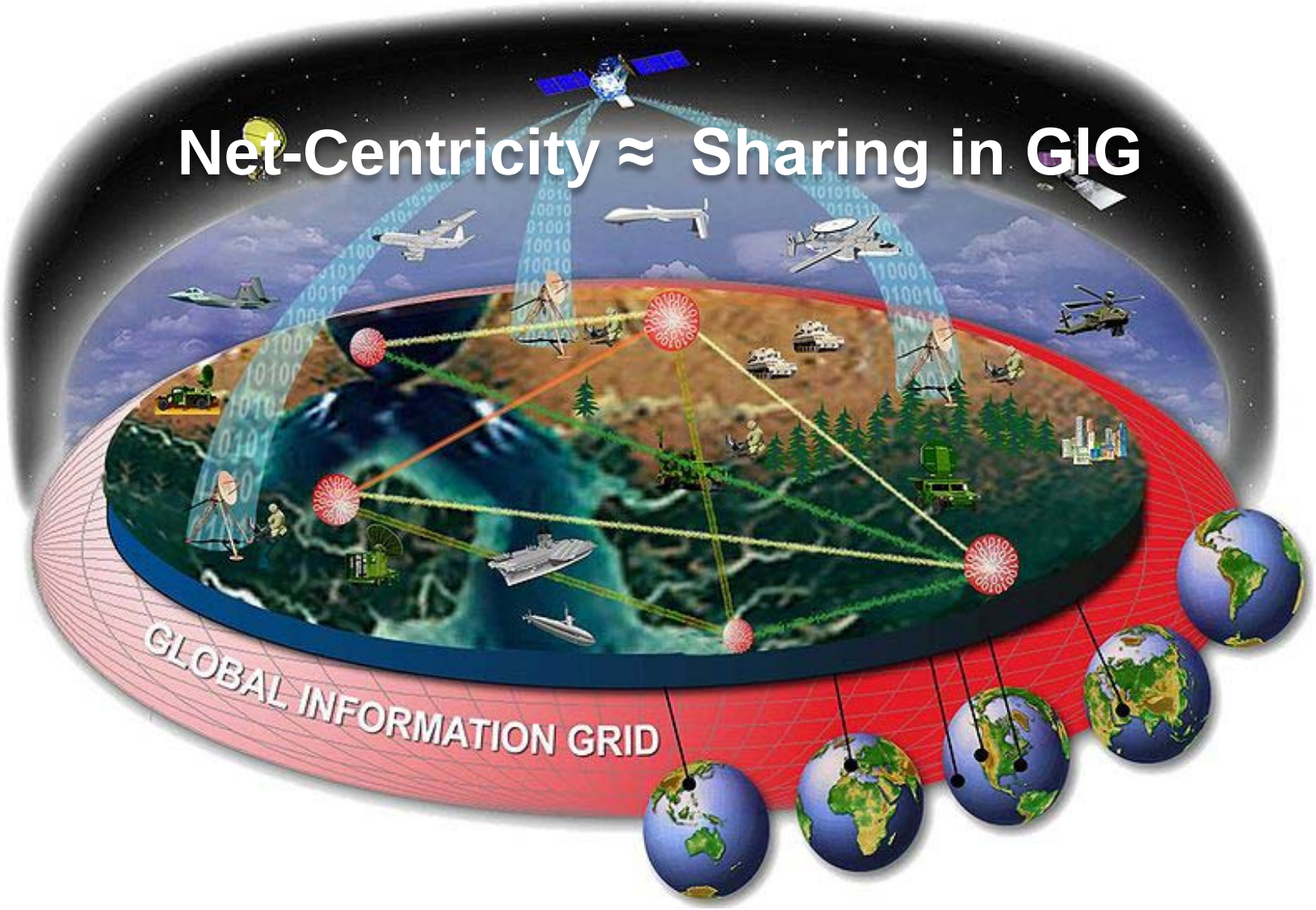
Net-Centric Updates and Case Studies

Oct 28, 2009

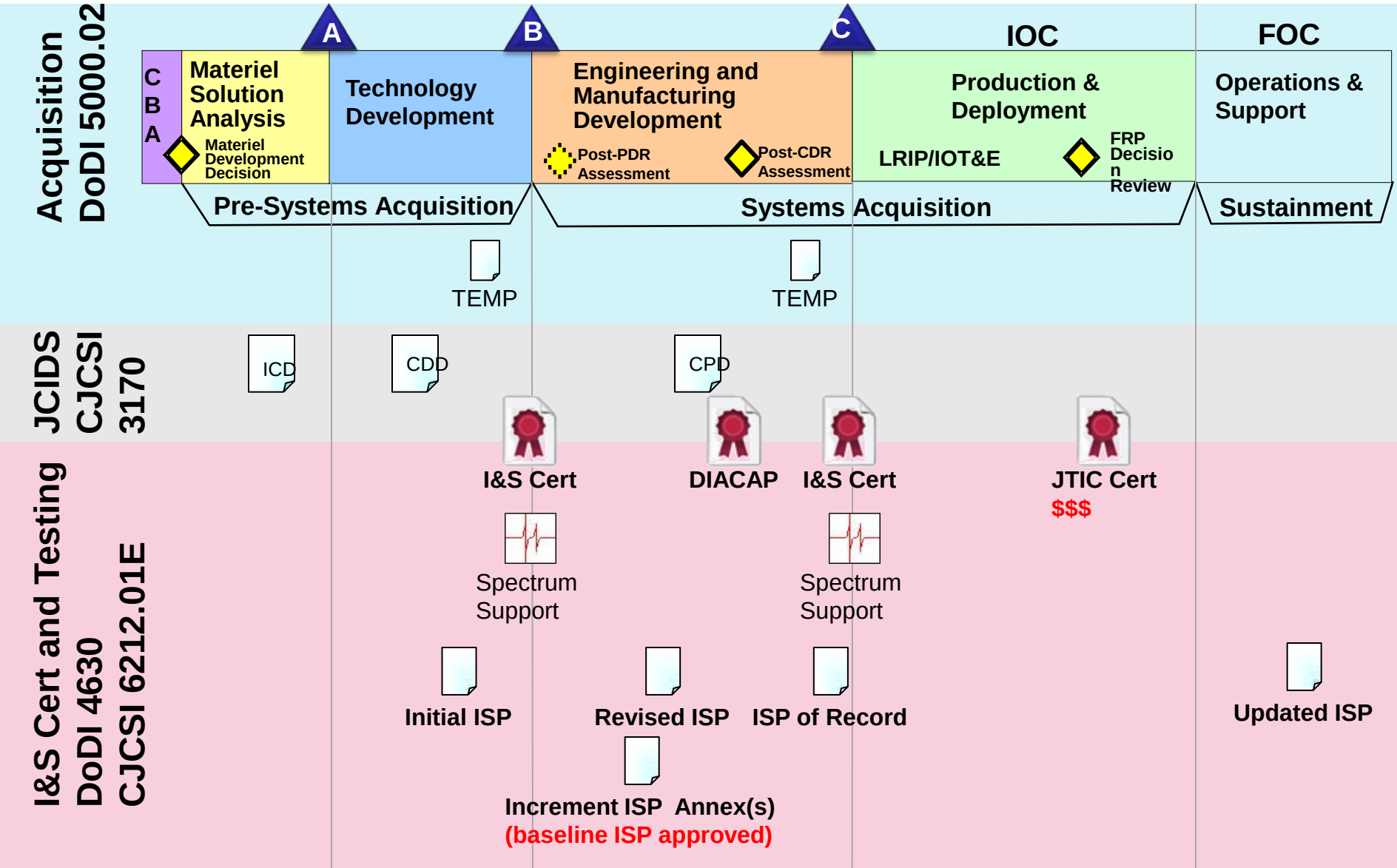
Donald Way
Lattice Government Services
619-553-7954
don.way@us.army.mil
dway@latticeincorporated.com

Hiekeun Ko, PhD
SPAWAR Systems Center Pacific
619-553-8013
hiekeun.ko@navy.mil

What is DoD Net-Centricity



Impacts on the DoD Acquisition



Net-Centric Compliance is Challenging

Policies

- DoDD 8320.02
- CJCSI 3170G
  - NR-KPP
- CJCSI 6212E
- DoDI 4630.8
- DoDD 8500.1
- JROCOM 130-08
- UCore

Strategies

- NC Data Strategy
- NC Service Strategy
- NC IA Strategy

Architectures

- DoD IEA
- DoDAF 1.5
- DoDAF 2.0
- UPDM
- JCSFL

Tests

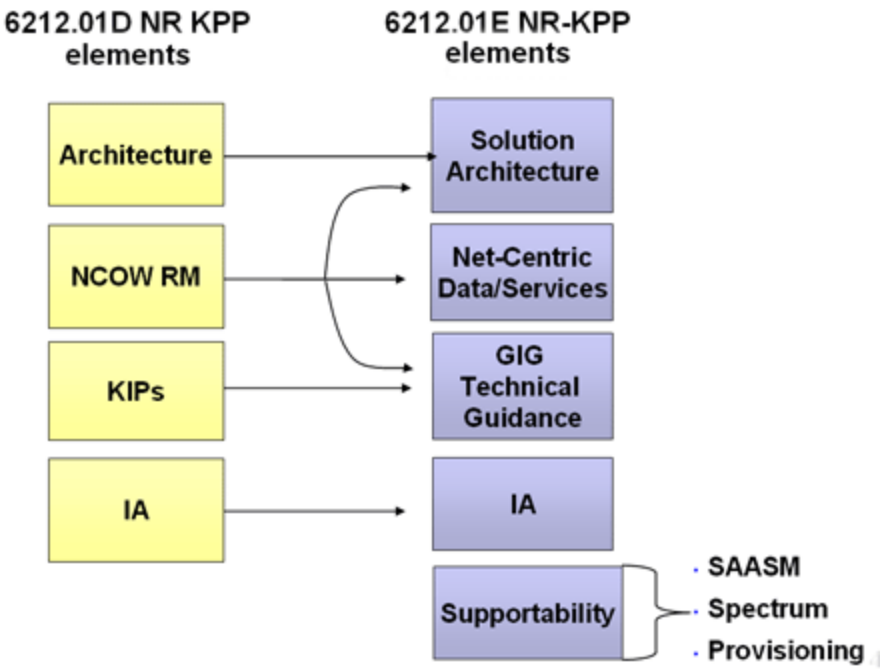
- JITC
- DICE
- JUICE
- CWID

Tools

- JCPAT-E
- DISR Online
- GTG Federation
- EISP
- DARS
- NCES
- MDR
  - DDMS

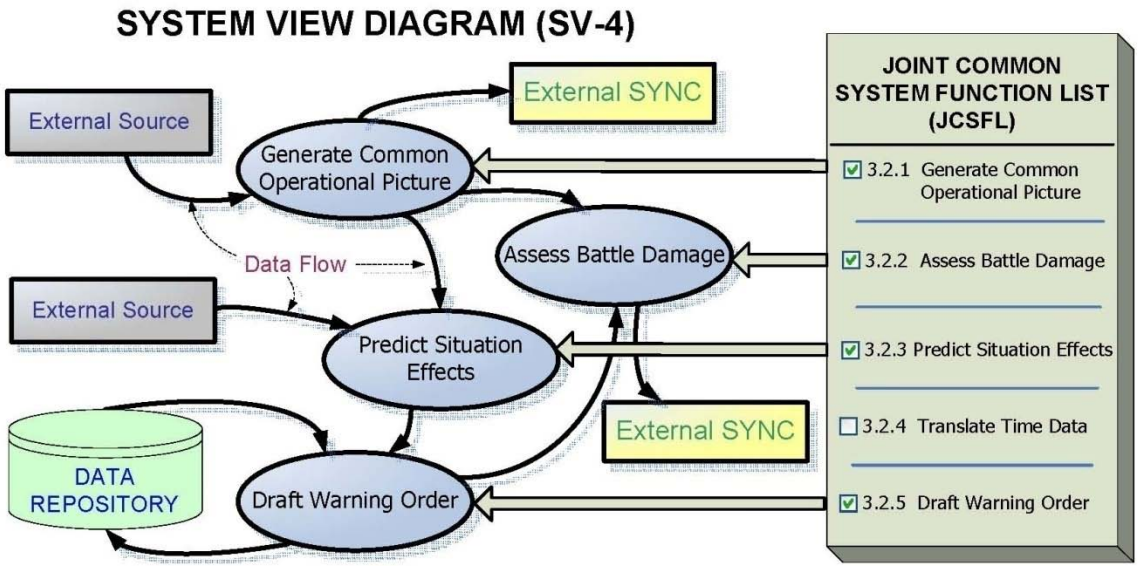
Net-Centric from CJCSI 6212.01E

Evolution of the Net-Ready Key Performance Parameters (NR-KPP)



Net-Centric Architecture

- Shifting from “Product-Centric” to “Data-Centric”
- Net-centric architecture compliance governed by **DoD IEA** business rules
- “All Views” (AV-1) diagram, must conform to DOD IEA standards and be maintained in the **DOD Architecture Registry System (DARS).**
- Introduces GIG Technical Guidance (GTG) as an emerging source for standard implementation (TV-1 and TV-2).
- Prescribes the use of JCSFL to describe functionality in a common lexicon.



Net-Centric Data Strategy

- Visible
- Accessible
- Understandable
- Institutionalized
- Trusted
- Interoperable
- Responsive to user needs

Net-Centric Service Strategy

- Provide
- Use
- Govern
- Monitor & Manage

Net-Centric Data / Service Exposure

Data Exposure Status Criteria

1. Visible
   a. DDMS entry in an Enterprise Catalog
   b. Content search function that federates to NCES Federated search
2. Accessible
   a. Policy
      i. Written policy for transparent access to data
      ii. Policy addresses access from Federated Search
   b. Operational (Transparent Access)
      i. Federated Search results provide active link
3. Understandable
   a. Enterprise Search
      i. Search terms/keywords appropriate for Mission area or data type
      ii. Described data understandable to both anticipated and unanticipated user
      iii. Mission data maps back to search terms

Service Exposure Status Criteria

1. Visible
   a. XSD & WSDL in DoD Metadata Registry (MDR)
   b. Service end-points in Universal Description, Discovery and Integration (UDDI)
2. Accessible
   a. UDDI
      i. Transparent M2M access to operational data at the targeted security enclave
      ii. Service links to accessible WSDL definition
   b. Policy
      i. Written policy for transparent M2M access
      ii. Policy addresses unanticipated developer
3. Understandable
   a. Service Provider schemas & supporting documentation in MDR
   b. Service schemas conform to standard (COI approved) vocabulary

Service Registration/Discovery

Register Metadata
to MDR
- DDMS record
- XML Schema
- WSDL
- XSL

Service Developer

DoD Metadata Registry

MDR

Net-Centric Publisher
by MDR

NET-CENTRIC PUBLISHER

NCES Service Discovery
by SOA Foundation

NCES SERVICE DISCOVERY

Reviewer

NCES Enterprise Search

NCES Enterprise Catalog

Net-Centric Data / Service

- Design Net-centric data / services
  - Design effective information exchanges within and among declared COIs
  - Consider unanticipated users
- Implement Net-centric data / services
  - Reuse or leverage others
  - Implement and use core services (NCES SOA Foundation)
- Identify net-centric services and shared enterprise-level data
  - Verify that data and services are properly registered, visible, and accessible
  - Conformance testing for data / schema (e.g., proper XML format)
  - Verify correct provision and use of services / data and any related performance parameters (QoS, timeliness, etc.)
- Compliant with net-centric standards
  - SOA
  - XML, WSDL, SOAP, UDDI, etc

GIG Technical Guidance

- Establishes the policies and guidance to maintain a common technical foundation for the GIG throughout the DoD enterprise.
- GTG describes **GIG Enterprise Service Profile (GESP)** concepts and their relationship to operational requirements, as specified in the Capability Development Document (CDD), Capability Production Document (CPD), Information Support Plan (ISP) and technical views (TV).

- **DISA** recently introduced **GTG Foundation** (GTG-F) that facilitates, standardized, and streamlines the GIG Interoperability assessment process.
- **GTG-F** enables the gathering of compliance data including GIG Enterprise Service Profiles (GESPs), IT standards, guidance statements, metadata standards, and program data
- GTG-F makes the virtual ISP process more efficient by enabling **Enhanced ISP (EISP)** to feed ISP data into automated ISP Assessment Module (IAM)
- **GESP** Declaration (or KIP declaration, e.g., for pre-6212.01E documents) should be contained in CDD, CPD, ISP or NR-KPP package.

Net-Centric IA Strategy

- Protect Information
- Defend Systems & Networks
- Align GIG Mission Assurance
- Transform & Enable IA Capabilities
- Create an IA Empowered Workforce

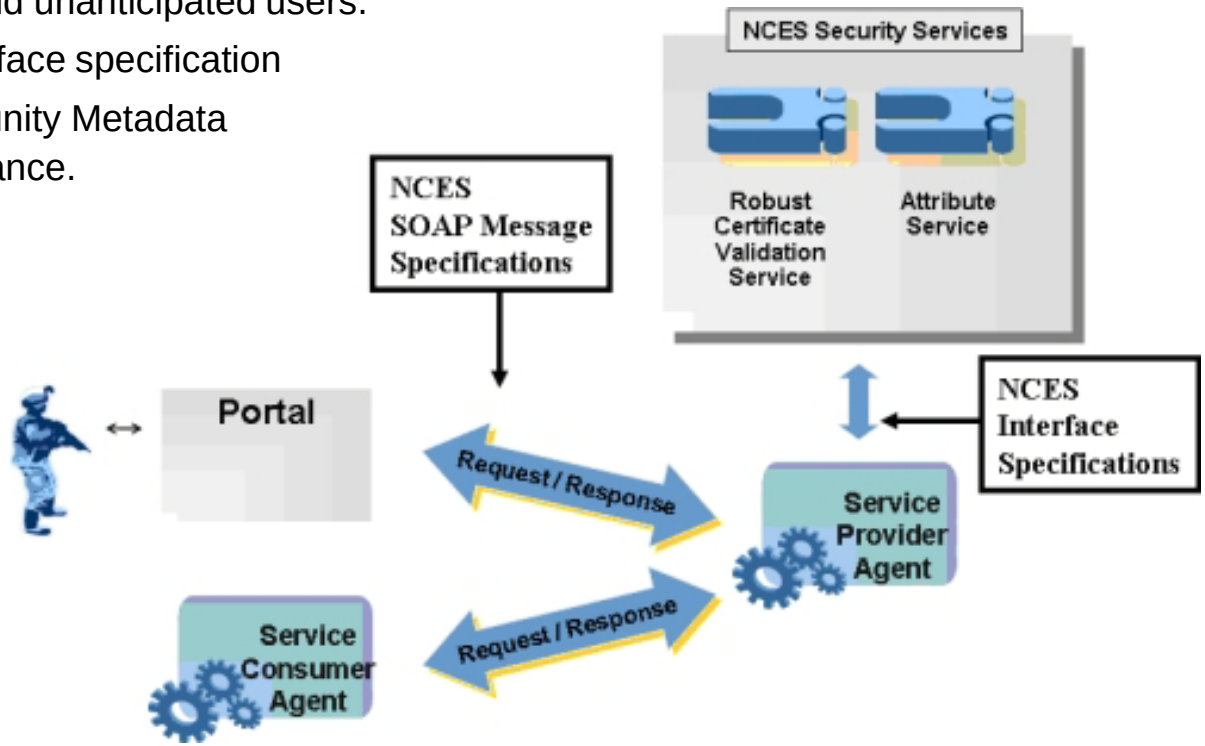
Net-Centric Service Security Standards

- Ensure security standards to protect service discovery by proper authentication and authorization mechanisms.
  - SOAP Security: WS Security, Industry (IBM, MS, and Verisign) and OASIS
  - Message Integrity: XML Signature, W3C
  - Message Confidentiality: XML Encryption, W3C
  - Access Control: XML Access Control Markup Language (XACML), OASIS

NCES – Core Enterprise Services

Service Security

- **NCES** provides the architecture for authentication, authorization, confidentiality, message integrity, non-repudiation, manageability, and accountability.
- Provides an enterprise Robust Certificate Validation Service **(RCVS)** to support effective authentication of both individuals and web services, with or without PKI.
- Provides an enterprise Attribute Service **(AS)** to support centralized retrieval of authoritative attribute values for individuals and unanticipated users.
- Provides a SOAP message interface specification
- Conforms to Intelligence Community Metadata Standards for Information Assurance.



Net-Centric IA

Accreditation / Certification

- Development Test stage
  - Verify the DIACAP process has been accomplished.
  - Review the System Identification Profile (SIP), Certification Report, Plan of Action and Milestones (POA&M) and the IATO, as applicable.
- Operational Test stage
  - Review the Comprehensive DIACAP Package.
  - Test configuration must mirror approved operational configuration (i.e., testing in a realistic IA environment)
  - Review OT report and verify IA compliance, as appropriate.
- Collect results of any IA accreditation, waivers, etc. for reporting in certification

Interoperability Testing

More emphasis on Integrated and Federated Testing

JITC

- **JITC** reviews testing already conducted as well as assessments prepared by independent testing organizations.
- **JITC** often performs its own testing and forwards test results to the Joint Staff, who validate the system's certification.
- Systems are generally certified for three years, after which they must be re-certified.

DICE

- JITC conducts **DoD Interoperability Communications Exercise (DICE)** in support of DoD Joint Interoperability testing, training, and exercise transformation initiatives 3 times per year.
- **DICE** is sponsored by the Joint Staff and U.S. Joint Forces Command (USJFCOM) and conducted by JITC

JUICE

- **Joint Users Interoperability Communications Exercise (JUICE)** formed in 1993 to answer the Army Secretary of Defense requirement for an organization to focus on Joint Interoperability across the DoD.
- Conducted by the Executive Agent Theater Joint Tactical Networks **(EA-TJTN)**
- Includes operational units, system developers, test and experimentation activities, life-cycle engineering organizations, and vendors) to examine and assess joint user-system interoperability in a robust simulated joint-task-force network functioning in a deployed environment.

Interoperability Test Events

- **Federated Test Events:** Testing shall include, when feasible, system-of-system and family-of-system (federated) live events to complete interoperability certification.

- **Federated Networks:** Maximum use of federated testing on federated networks (DREN, DISN, NIPR, SIPR) and federated tracking through the **Federated Development & Certification Environment (FDCE)** should be employed.

Leveraging operational tests:

- Interoperability tests of **Joint Mission threads** should be integrated throughout operational Testing. 6212.01E authorizes the use of Operational Assessments and Evaluation Reports (OAR/OER) to evaluate the operational effectiveness and validation of interoperability requirements.

- **JITC** reviews testing already conducted as well as assessments prepared by independent testing organizations. JITC often performs its own testing and forwards test results to the Joint Staff, who validate a system's certification. Systems are generally certified for three years, after which they must be re-certified.

Net-Centric Assessment
by JPEO-CBD Software Support Activity

- Identifies critical net-centricity items to assess the program during “Pre-Milestone C”
  - Program Schedule (Integrated Master Schedule (IMS) and detailed schedules as available)
  - DD 1494 Spectrum Supportability Certification OR Plan And Justification For Submission To USD(AT&L), ASD(NII), DOT&E, and The Chair, MCEB
  - Capability Production Document (CPD)
  - Updated NR-KPP
  - Certification and Accreditation Process Plan
  - J6 I&S Certification
  - Military Communications-Electronics Board **(MCEB)** Interim Certificate To Operate (ICTO) Request
  - Detailed Architecture Products Consistent With DoDAF Requirements
  - The Program RFP and Performance Specification
  - Database Creation Scripts For All Developed Databases
  - Interface Requirements Specification (IRS)

Net-Centric Assessment (con't)

- Mapping document that maps the program's data exchange requirements to a common **Data Model** or conforming **XML Schema**
- List of entities and attributes or XML types currently used by the program.
- **OV-7** and **SV-11** logical and physical data models
- All **XML** Schema files, including subsets.
- Web Service Description Language **(WSDL)** files for all defined Web Services
- All XML documents created/logged during system testing
- Signed System Security Authorization Agreement OR DIACAP derivative
- Signed Interim/Approval To Operate (I/ATO) letter
- Signed **Clinger-Cohen Act (CCA)** compliance statement, if required
- Signed Information Support Plan **(ISP)**
- Signed Cross Domain Appendix (CDA) (if required)
- Systems Engineering Plan **(SEP)**

Net-Centric Updated Resources

Best Sources of Standards and Information

- DAU Acquisition Community Connection
  - https://acc.dau.mil
- NCES Developer Community on DKO
  - https://www.us.army.mil/suite/kc/6998357
  - Is the best resource for the current concepts, direction and information on the Net-Centric initiative
- NESI-X
  - Net-Centric Enterprise Solutions for Interoperability () site at http://nesipublic.spawar.navy.mil/nesix/Frames, is a complete resource. Among other things the site offers developer support, guidance and best practices.

Case Study:
CBRN Data Model

- **The CBRN data model** is a realization of the **DoD net-centric data strategy** (NCDS) and facilitates interoperability and reuse by specifying a common data structure through the **CBRN COI.**
- **The CBRN Data Model** includes standardized, common, open tagged metadata in accordance with the Department of Defense **Discovery Metadata Specification (DDMS).**
- Developed using the Integration DEFinition for Information Modeling 1 eXtended (IDEF1X) format, as specified in the **Department of Defense (DoD) Information Standards Registry (DISR).**
- Lays the foundation for the creation of **XML tags** and schemas and assists in data quality checks for syntactic and logical consistencies. These XML tags to the CBRN namespace, and are registered in the DoD MDR.
- Built upon the North Atlantic Treaty Organization (NATO) **Joint Command and Control Information Exchange Data Model (JC3IEDM).**
- Expands the **JC3IEDM** to reflect all **Allied Tactical Publication (ATP) 45** NATO Nuclear, Biological, Chemical (NBC) message sets and related information elements.
- **CBRN Data Model v1.9** (2009) includes 569 entities, 5067 attributes, and 1811 physical relationships.
- **POC: Ms. Sheila Vachher**

  JPEO-CBD SSA Data Management, 703-933-3336, savachher@alionscience.com

Case Study:
CBRN Data Model (con't)

Other Benefits:

- Facilitates a common CBRN Domain Representation
- Enables Data Interoperability & Re-use
- Facilitates Interoperability:
  - Scalable and extensible
  - Specifies meaning and structure of data
  - Specifies relationships among data
  - Provides open standard basis for Data Exchange XML.
- Release 1.9 pilots the use of **Geospatial Markup Language (GML)** in the CBRN XML Schema Definition (XSD). **GML** is the mandated standard for geospatial representation in DoD IT Standards Repository (DISR) and in the **Universal Core (UCORE).** Still **GML** and **UCORE** have yet to be adopted into developing technologies by the greater DOD community. **Data Harmonization** efforts include:
  - Harmonization with the CBRN Common Sensor Interface **(CCSI),** ANSI N42.42, IEEE 1451 and OGC Sensor Web Enablement to include: Observations & Measurements, SensorML and TransducerML.
  - Defense Threat Reduction Agency **(DTRA)** and JPEO-CBD harmonization of Radiological / Nuclear data.
  - Harmonization with Department of Homeland Security **(DHS)** Chemical and Biological Alarm Summary.

Case Study:

CBRN Data Model (con't)

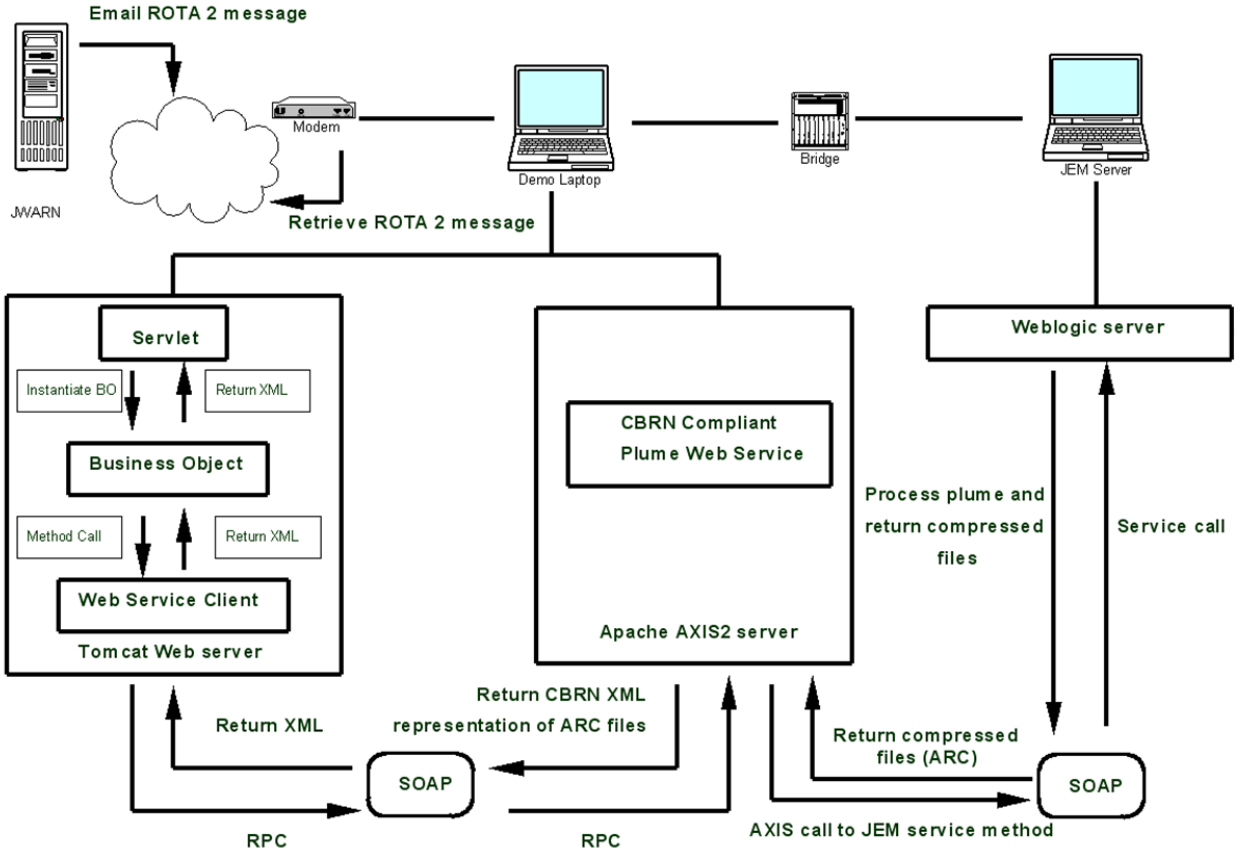


Diagram depicts the flow of a CBRN message through a data model compliant transformation in a web-server agnostic, SOA based system.

Case Study:
Joint Effects Model (JEM)

JEM Overview and Web Service Implementation

- **JEM** is a software simulation system employing advanced atmospheric transport and dispersion models to create high fidelity, hazard predictions of chemical, biological, radiological, and nuclear **(CBRN)** toxic materials to protect from airborne contamination.
- A web-based application utilizing **Web Services** in an **SOA** leveraging open eXtensible Markup Language **(XML)** -based standards and transport protocols to exchange data and encapsulate behaviors.
- Utilizes the Web Services Definition Language **(WSDL)** to expose service functionality and enable interoperation with various Weather and Visualization Services.

JEM's Net-Centric Weather Service

- **JEM** is capable of requesting, receiving and manually inputting meteorology and oceanography **(METOC)** data from local and strategic sources including: the Joint Weather Impact System **(JWIS, Air Force)** and the Defense Threat Reduction Agency's (DTRA) **METOC** Data Service **(MDS).**
- Within its delivery software for both **JWIS** and **MDS, JEM** communicates using the Host Name, User ID Name, User Password and Port Number; which allows immediate access to weather data via the NIPRNET and SIPRNET.
- **JEM** is one of the first applications to employ **JWIS Web Services**, that employs the METOC COI **Joint METOC Broker Language (JMBL)** as the XML interface and will also employ the **Joint Environmental Toolkit (JET).**

Case Study:

JEM (con't)

JEM Modeling Web Service

- **JEM** provides **modeling services** to other applications.
- The JEM **Modeling Web Service** acts as the intermediary between external applications and the JEM modeling application.
- Applications such as **JWARN** can request information and services from the Modeling Service using **SOAP** messages over **HTTPS**.

- **JEM Modeling Web Service** allows clients to submit modeling requests, check status of submitted jobs, and retrieve calculation results.

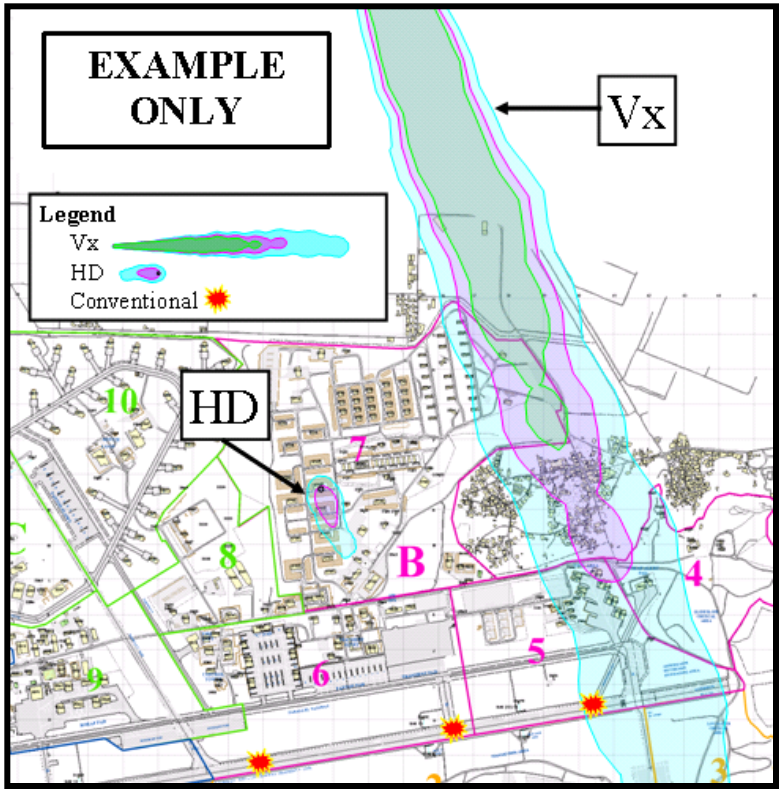
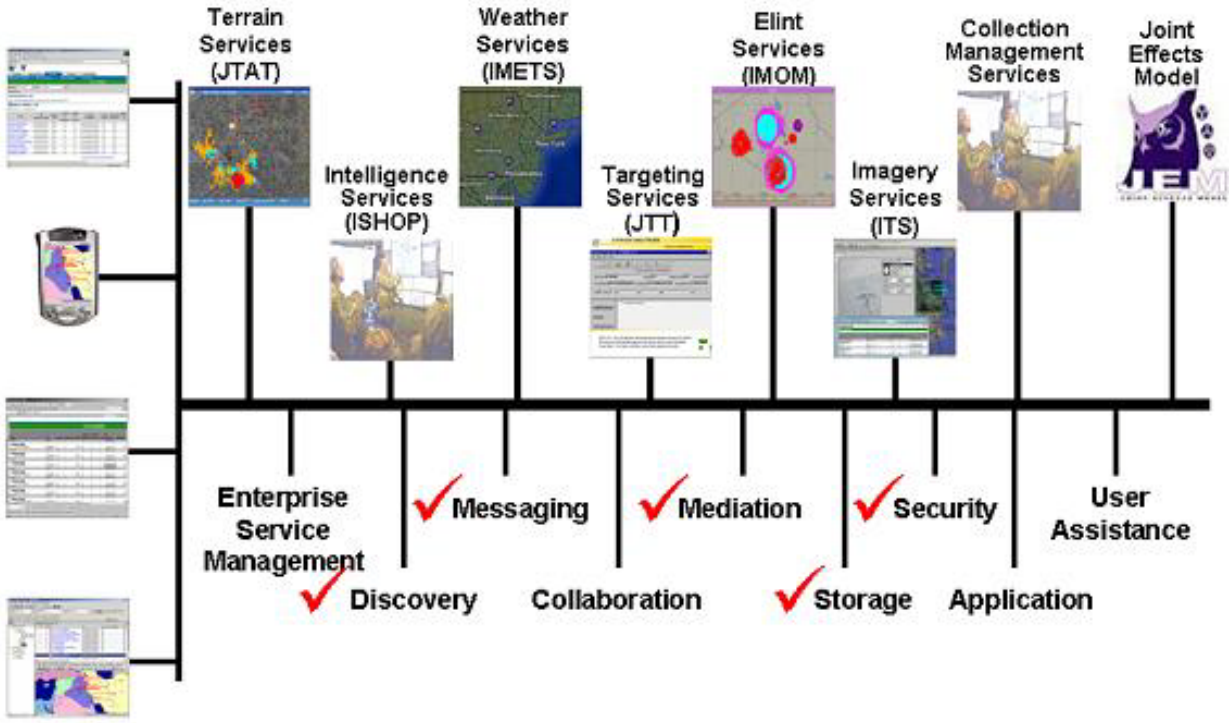


Diagram depicts a "Plume Model" generated from the JEM Modeling Web Service

Case Study:
JEM Web Service Relationships



Above describes the JEM's relationship to other peer applications that can utilize the JEM Modeling Service.

Case Study:
JEM Best Practices

- **Best practices in Net-Centric Development:**
  - A **CBRN Community of Interest (COI)** was developed along with an XML namespace (designed to DOD data and metadata standards) and registered with in **DOD Metadata Registry (MDR)**.
  - **JEM** is main contributor to **CBRN COI** and **CBRN Namespace**, also designed to metadata standards and registered in the MDR.
  - **JEM** is designed to be server "agnostic". For Instance, JEM is hosted via the Battle Command Common **Services (BCCS)** platform, using an open-source/**JBOSS** configuration and is deployed on **GCCS** using **BEA's Web Logic** application framework.
  - Test Interoperability with systems calling a JEM Web Service Interface "early and often".
  - Designed to orchestrate multiple weather services in combination.

- **Best practices in Net-Centric Certification:**
  - Execute early and consistent contact with the **ASD/NII** staff to ensure that ISP development is in line with what was is expected by **J-6** and **J-3**
  - Promote tight coordination/ feedback loop with **JRO** engineers in **OV diagram** preparation**.**
  - Ensure that staff is skilled and has sufficient background to perform the required work.
  - Respond quickly to **JCPAT** feedback to keep process moving forward without delay.

Case Study

Joint Warning and Reporting Network (JWARN - Increment 1)

What is JWARN?

- **The Joint Warning and Reporting Network (JWARN)** is a fully fielded I&S and V&V completed software application that provides Joint forces with a comprehensive analysis and response capability to minimize the effects of Nuclear, Biological and Chemical **(NBC)** attacks.

- **JWARN** is also used in response to accidents and incidents involving Toxic Industrial Chemicals **(TICs)** and Toxic Industrial Materials **(TIMs)**.

- **JWARN** Enables an immediate and integrated response to threats of contamination by weapons of mass destruction through rapid warning and dissemination of Chemical, Biological, Radiological and Nuclear **(CBRN)** information.

Case Study

Joint Warning and Reporting Network (JWARN - Increment 1)

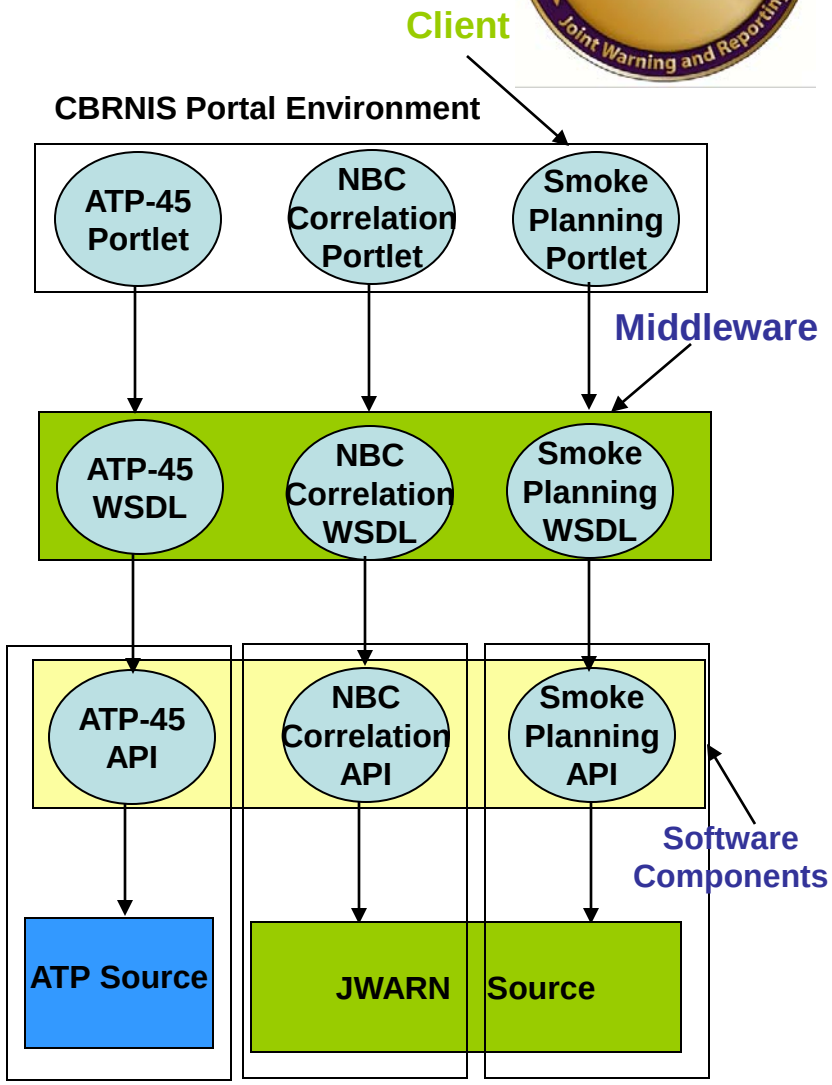
JWARN Functionality:

- Collects, generates, edits, and disseminates **NBC reports** and plots and provides a means of ensuring all addressees have received a sent message
- Provides application support for; **GCCS-M, GCCS-AF, GCCS-A, GCCS-J, FBCB2** (via message exchange) **and MCS, C2PC/JTCW**.
- Allows **NBC** reports (NBC-1/NBC-4) to be formatted and transmitted within 2 minutes and allows operator selection of automatic, delayed, or on-command sending of NBC reports
- Provides automated **sensor** interfaces for **M22(ACADA), ADM-300, AN/VDR2, M8A1, M21(RSCAAL), JSLSCAD, JCAD, JBPDS.**
- **Current Status: JWARN 1F (Block 1)** includes a worldwide distribution to all Theatres, Services and Bases and supports exercises in South Korea, Afghanistan, Iraq and within NATO activity areas.
- **JWARN Product Support provides:** Training events, Computer-Based Training, Quick Reference Guides for each C2 host and a 24/7 Call Center/Help Desk.

Case Study
Web-Enabled JWARN (WEJ)

JWARN Future Development of Web Enabled JWARN **(WEJ)** is to include full Net-Centric Interoperability and the following enhancements:

- **Cost Savings**
  - Facilitates code reuse.
  - Better adapts to changing environments.
  - Limited support required to deploy, field and train.
  - Easier to certify and test single component vs system. Process can also be automated.
  - Training costs are lower as web-based applications.
  - Administration costs are much lower since a limited number of servers need be maintained
- **Performance Improvements**
  - Utilizing load-balancing through server-side flexibility and scalability also greatly improves performance at minimal cost.
- **Ease of Use**
  - Consolidation of information can be delivered throughout the entire organization at any time and from any location in the world.
  - Decision makers can obtain information in real time.



Case Study

WEJ with ATP-45

What is ATP-45?

- A messaging format standard based on standard **NATO Allied Technical Publication ATP45** procedures used by CBRN hazard prediction software including JWARN and JEM.
- Allows the display NBC hazard areas resulting from the use of NBC weapon systems and dissemination devices over a geographic area. Creates a “plume” model.
- Is currently being updated to meet the latest dynamic technology and force protection requirements.
- The next version **ATP-45 Delta (D)** has been requested for delivery by December 2010**.** Current version is **Bravo (B)** and services have yet to adopt ATP-45 **Charlie (C)** versions.

Problems:

- Services and C2 Systems are slow to adopt new ATP-45 versions so CBRN applications must easily adapt to various C2 / ATP configurations. JWARN/JEM software must be “backward” compatible with MCS, FBCB2, C2PC, GCCS all legacy ATP-45 versions.
- For Instance, version **JWARN IF (Block 1)** uses an older version of the ATP-45 algorithm.
- Interfaces to this **ATP-45** algorithm (Bravo or Charlie) are tightly coupled to the data structures of each application and **Input AND Output Parameters (fields)** are also different.
  - –Bravo (JWARN Block 2) uses: **complex Report Object**
  - –Charlie (BNI demo code): uses: **actual “/” delimited AdatP3 string format**

Case Study
WEJ / ATP-45 (con't)

Solution:

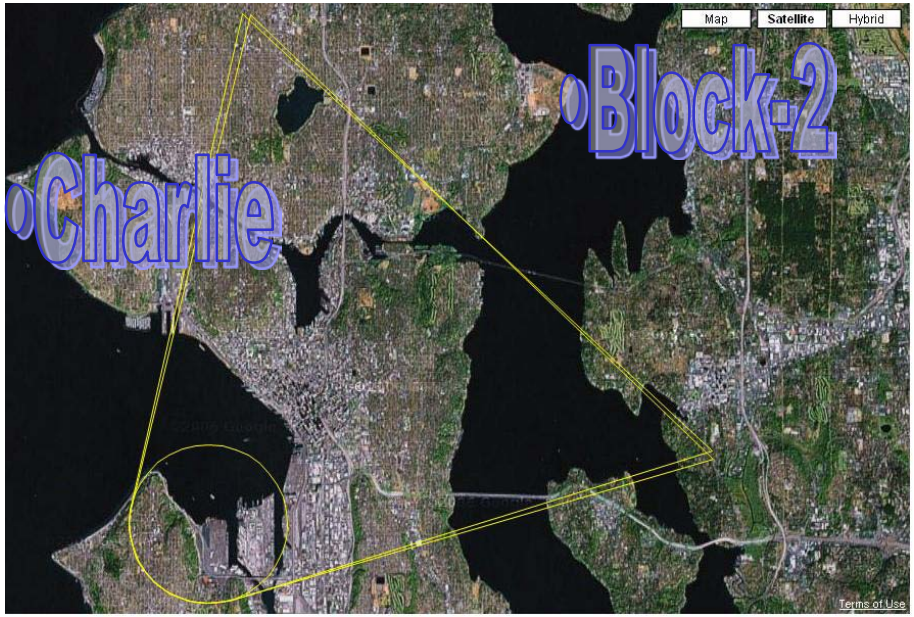
The ATP-45 Calculator Service Component was incorporated into the **WEJ** Hazard Prediction Service during software design and development. This calculator service supports backward compatibility and enables quick switching between various ATP-45 versions.

Hazard Prediction Components include:

- Get ATP-45 Bravo Hazard service.
- Get ATP-45 Charlie Hazard Service.

Planning/Calculation Components Include:

- Route Planning Service.
- Nuclear Planning Service.
- Smoke Planning Service.
- Flame field Expedients Planning Service.



This figure shows the results of both Bravo (Block-2) and Charlie (BNI) ATP-45 Calculations.

Case Study:
JEM / ATP 45

Problems:

- **JEM (B6P6**) used an older version of the “same” ATP-45 algorithm than JWARN (B321)
- Different versions of **JEM** called different versions of ATP-45 Bravo and Charlie algorithms

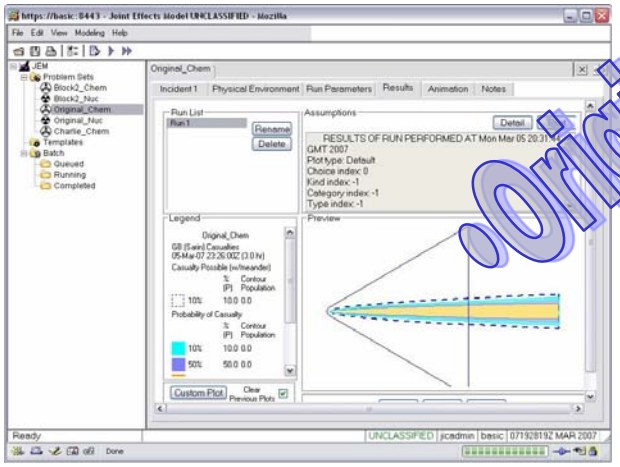
Solutions:

- Modifications to two java files that access common component rather than specific files (as is the older implementation)
  - Modification to build script in order to keep the ATP-45 service (application jar file) separate from the JEMSC.jar (data connector jar file)
  - Usage of a properties file to “switch” between algorithm versions at run-time rather than having to make code changes and recompile.
  - The **JEM code (B6P6)** was then updated to call this new API.
  - The **WEJ** project also developed a hazard prediction service which uses the ATP-45 algorithm. The corresponding code that calls this new API was also updated.

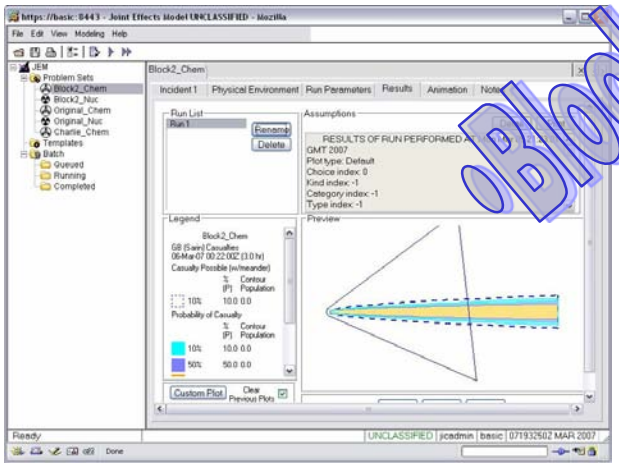
Case Study:
JEM / ATP 45 (con't)

Solutions: (con't)

– The newly created component allowed the software to "substitute" calls to the **ATP-45 C** version of the algorithm (received as demo code from BNI) by adding an implementation of the interface for the new version.
– A properties file was also added so that this "switch" could be accomplished at run-time rather than having to edit / recompile the application.



JEM - Original Chem Hazard



JEM - Bravo (Block-2) Chem Hazard

Summary

- Start a new or join an existing Community of Interest (COI).
- Become familiar with latest NCES and GTG information and offerings.
- Coordinate Testing with JITC early and often while leveraging operational tests and federated test event.
- Apply new standards approximately six months after they are formally introduced into compliance documentation.

Case Study Summary:

- CBRN Data Model facilitates interoperability and reuse by specifying a common data structure through the CBRN COI.
- JEM successfully obtained Interoperability with other systems by constantly calling their Net-Centric Web Service Interface during frequent and ongoing tests.
- A Net-Centric ATP-45 Calculator Service Component was incorporated into the WEJ Hazard Prediction Service during software development, allowing agile backward compatibility.
- JEM developed common components to switch between algorithms at runtime.

Acronym Lists

- CBRN – Chemical Biological Radiological and Nuclear
- CCA - Clinger-Cohen Act
- CDD – Capability Development Document
- COI - Communities of Interest
- CPD – Capability Production Document
- DARS – DoD Architecture Registry System
- DDMS – DoD Discovery Metadata Specification
- DIACAP - Defense Information Assurance Certification and Accreditation Process
- DICE - DoD Interoperability Communications Exercise
- DISR - DOD Information Technology Standards Registry
- EISP – Enhanced Information Support Plan
- GESP – GIG Enterprise Service Profile
- GIG – Global Information Grid
- I&S – Interoperability and Supportability
- ICD – Initial Capability Documentation
- ISP – Information Support Plan
- JC3IEDM - Joint Command and Control Information Exchange Data Model
- JCSFL – Joint Common Systems Function List

Acronym Lists (con't)

- JEM – Joint Effects Model
- JTRS – Joint Tactical Radio System
- JUICE - Joint Users Interoperability Communications Exercise
- JWARN – Joint Warning and Reporting Network
- METOC – Meteorology and Oceanography
- NCES – Net-Centric Enterprise Services
- NR-KPP – Net-Ready Key Performance Parameter
- SAASM – Selective Availability Anti-Spoofing Module
- SOAP – Simple Object Access Protocol
- TICs – Toxic Industrial Chemicals
- TIMs – Toxic Industrial Materials
- UDDI - Universal Description, Discovery and Integration
- UPDM – Unified Profile for DoDAF/MODAF
- XML - eXtensible Markup Language
- WEJ - Web Enabled JWARN
- WSDL - Web Service Description Language