



Utilizing Architecture Data in the Enhanced Information Support Plan (EISP) Process

**DoD EA Conference Brief
San Antonio, TX
13 May 2010**

Ed Zick
DoD CIO (SP&IM)
(703) 601-4729 ext. 115
edward.zick@osd.mil



Purpose of the Brief



- To describe how the:
 - Information Support Plan process utilizes architecture data
 - Enhanced Information Support Plan (EISP) has automated the analysis of that data
 - plans for transitioning the EISP to a web-based capability will allow authoritative data to be imported and shared with other organizations and processes



Information Support Plan (ISP) Background

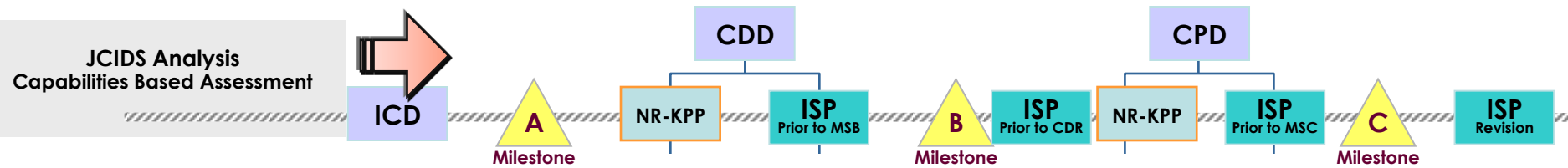


ISP Purpose:

- The ISP identifies potential *information support* implementation *issues and risks* that, if not properly managed, will *limit or restrict* the ability of a *program to be operationally employed* in accordance with requirements.

Content:

- Identifies the program's *processes* that drive information requirements
- Analyzes the program's *critical information dependencies and sources* in supporting the identified processes
- Assesses the program's path toward becoming *Net-Centric*
- Describes the program's *Information Assurance* compliance
- Describes the program's *Frequency Spectrum* dependencies





Enhanced ISP (EISP) Development Philosophy



- Transitions the legacy ISP process from document-centric to *data-centric*
- Allows data entry through *formatted templates* that *focus* the user on the program's *processes* and *critical information* dependencies to ensure that requirements are being met in compliance with DoD CIO policy and guidance
- Extensible Markup Language (XML) *tagging of data* for reuse is *transparent* to the user
- Collects *data in context* while *applying analysis and business rules* that help to drive decision making and allows *follow-on analysis* by other users and processes

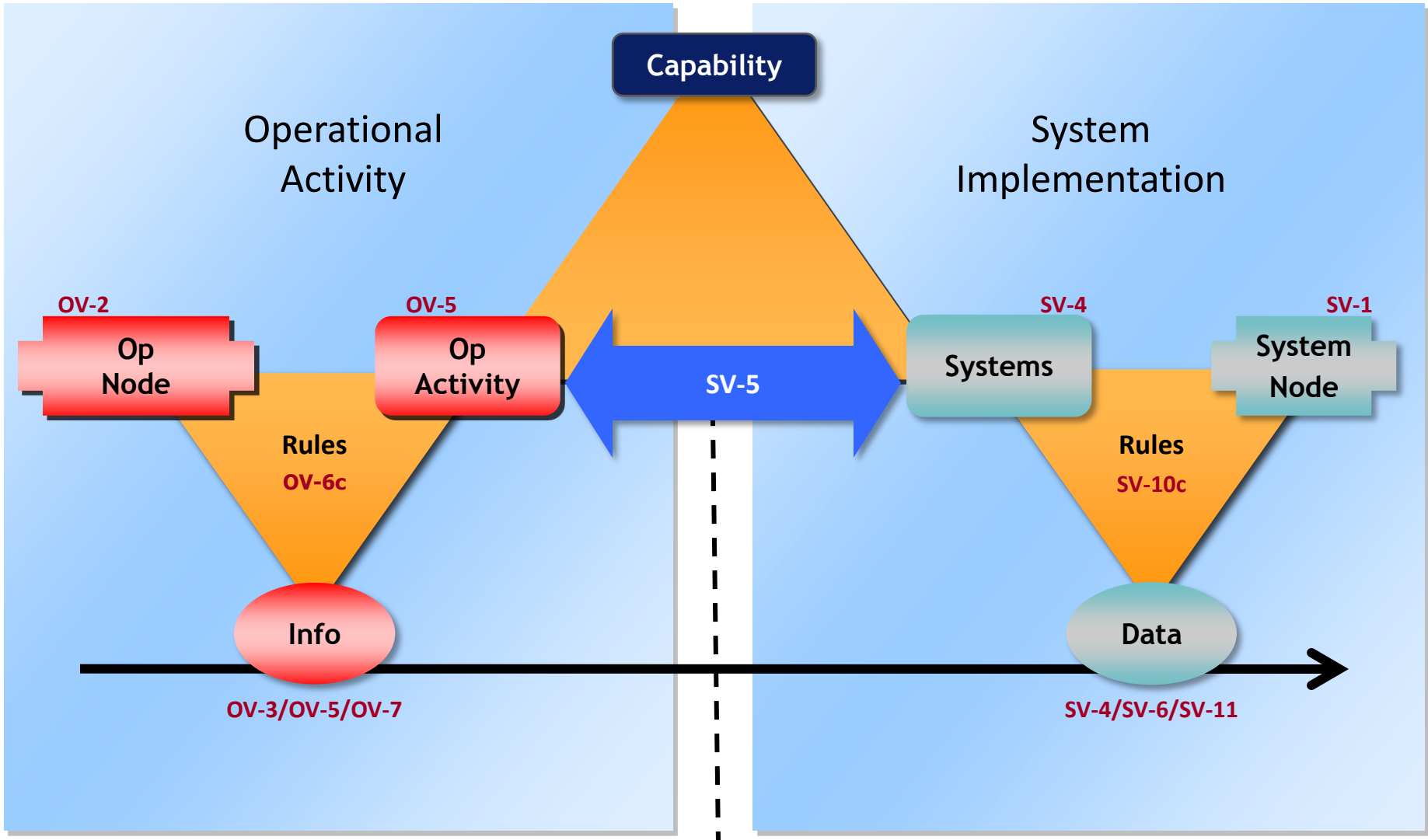
EISP Version 1.03 and Version 2.0 User Community Snapshot

EISP Downloads	700+
Program Offices using EISP	100+
Submitted EISPs for Joint Level Review	25+

The Stryker Brigade Combat Team (SBCT) Program Office estimated a 30-40% reduction in labor costs for each ISP created using the EISP methodology

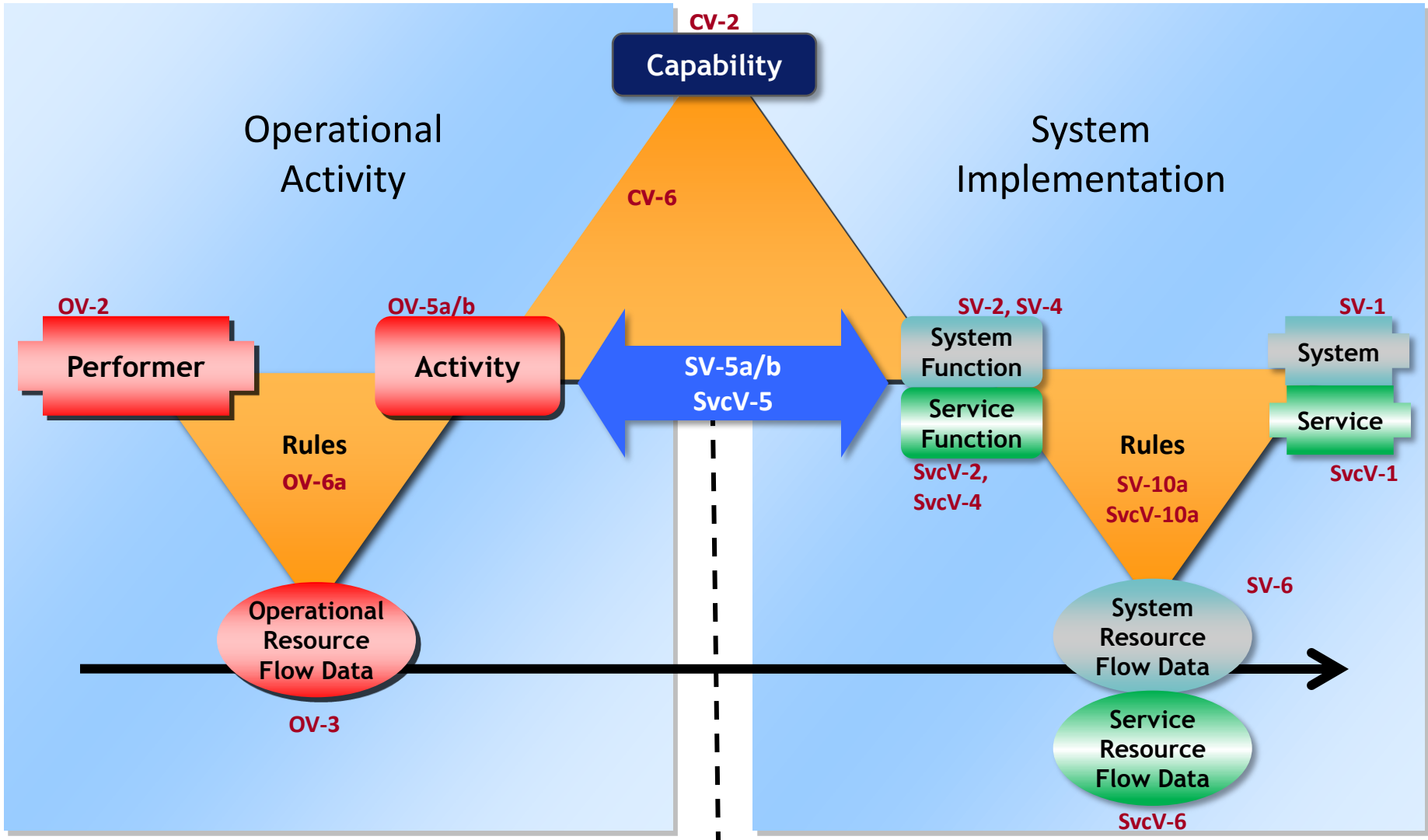


DoDAF 1.5 Products in the EISP





DoDAF 2.0 Products in the EISP

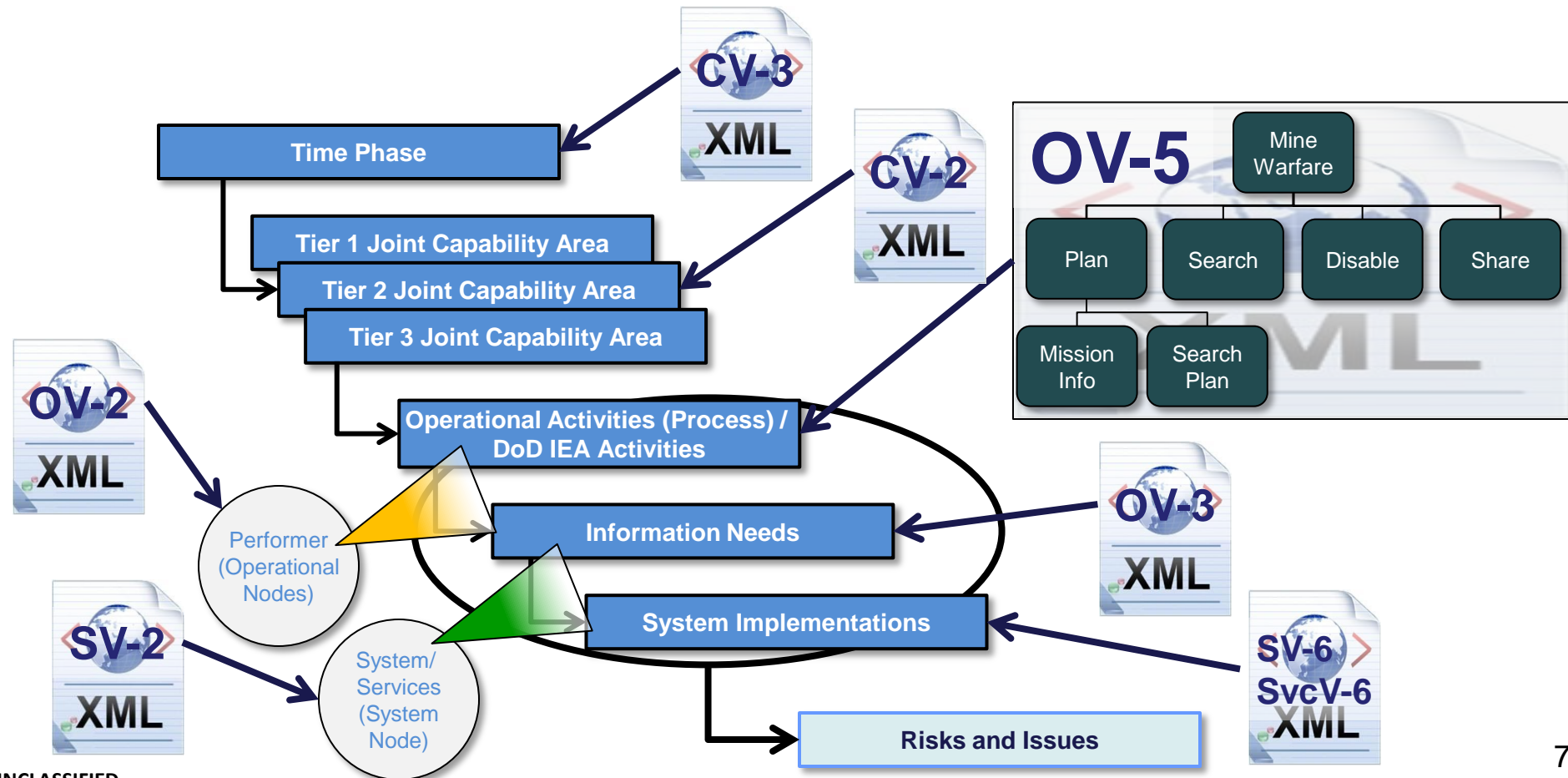




The EISP Analysis Process



- In the Process Analysis section, the ISP developer is asked to enter their detailed warfighter or business process related data
 - The information for these sections is drawn directly from their existing architecture products

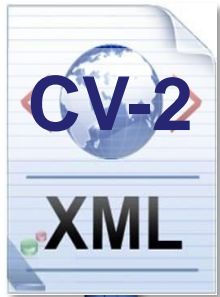




Process Analysis: Joint Capability Areas (JCAs)



- Joint Capability Areas (JCAs) are used to bin a program's capabilities and activities utilizing a standard framework
- Cross program analysis can be conducted based on programs with similar JCAs



The screenshot displays a software interface for configuring Joint Capability Areas (JCAs). On the left, a hierarchical tree structure is shown under 'Time Phases'. The tree includes 'IOC' and 'FOC' sections, each with 'Operational Nodes'. Under 'IOC', the path is: Tier 1 Joint Capability Areas > Force Application > Tier 2 Joint Capability Areas > Maneuver > Tier 3 Joint Capability Areas. The 'Tier 3 Joint Capability Areas' node is highlighted with a blue rounded rectangle. A blue arrow points from the 'CV-2 XML' icon to this highlighted node. The right side of the interface shows a configuration panel for a 'Tier 3 Joint Capability Area(s)'. It contains a text box with instructions: 'Enter the relevant Joint Capability Areas that are supported by the program. To add a new Joint Capability Area, right-click on the 'Tier 3 Joint Capability Area' bookmark in the Time Phases Tree and select 'Add Tier 3 Joint Capability Area.' Then, select the Tier 3 Joint Capability Area from the drop-down in the table. If the desired Tier 3 Joint Capability Area is not in the drop-down, select 'Other' and type in the name of the desired Joint Capability Area.' Below the text box is an 'Add JCA' button. At the bottom, a 'Joint Capability Area Summary' table is visible, containing one entry:

Tier 3 Joint Capability Area(s)	Joint Capability Area Name
Maneuver to Engage (MTE)	Maneuver to Engage (MTE)



Process Analysis: Activity Hierarchy



- After the Joint Capability Areas have been entered, the Activity Hierarchy is entered into the EISP
 - Activity Hierarchy contains Activities and Sub-Activities



The screenshot displays the EISP interface. On the left, a tree view shows the hierarchy: Time Phases > IOC > Operational Nodes > Tier 1 Joint Capability Areas > Force Application > Tier 2 Joint Capability Areas > Maneuver > Activities > Mine Warfare 1.1.1 > Sub Activities. The 'Search/Locate 1.1.1.2' activity is highlighted. A blue arrow points from this activity to the right-hand data entry form.

The data entry form is titled "Search/Locate for Mine Warfare" and contains the following fields:

- Task List Name: Navy TTP
- * Activity Number: 1.1.1.2
- * Activity Title: Search/Locate (circled in blue)
- Activity Description: (empty text area)

Below the form is a table with a header row "Text" and one data row containing "Searching for mines." A blue arrow also points from the "Search/Locate" activity in the hierarchy to the "Activity Title" field in the form.





Process Analysis: Information Need(s)



- For each Leaf Activity, indicate the associated Information Needs and Minimum Parameter information as required.

OV-5 Mine Warfare

- Plan
 - Mission Info
- Search
 - Search Plan
 - Position Of Mine
- Disable
- Share

Information Need Form Fields:

- Information Need Name: Position of Mine
- Information Need Source: ON 1.2 Communication Systems
- Information Need Consumer: ON 1.5 Mission Systems
- Information Need Identifier: IER 10
- Information Need Type: Input to the Process

Information Need Description:

To add a new paragraph, right-click on the table and select "Add" from the pop-up menu or click the row to add text. Each row in the table will appear as a formatted paragraph in the final output.

Text
This information need consists the position of the mine.

Parameters:

- This Information Need is Critical to this Activity and it is an external IER.
- Intelligence Supportability Related

Information Need Quality:

- Minimum Parameters
- Quality
- Quantity
- Timeliness
- Other

Callout Box: An Information Need's Minimum Parameters are defined here and are analyzed against the System Implementations associated with the Information Need





Process Analysis: System Implementations



- For each Information Need indicated, enter the System Implementation(s) that satisfies the Information Need and explain any potential issues or risks, if required.

System Implementation for Position of Mine

Enter the following regarding the System Implementations required to complete the Information Needs that have been identified in this section.

System Implementation Name: System Implementation for Position of Mine

Information Need Source: ON 1.2 Communication Systems

System Implementation Source: SN 1.3.3.1.1 RT-1794(C) AN/ARC-210

Information Need Consumer: ON 1.5 Mission Systems

System Implementation Consumer: SN 5.2 LAN

Transport Methodology: TCP/IP

Uses DISN Uses Wireless Capability

Data Sharing Characteristics

Tagged MDR (DDMS) Registered Web Service

Discoverable IPv6 Capable Other

Risks and Issues can only be added to system implementations when the parent Information Need is Critical, is Intel Supportability Related, or contains Minimum Parameters.

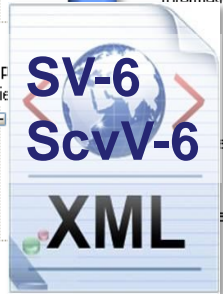
To add a Risk or Issue for a Critical or Intel Related System Implementation, right-click on the System Implementation bookmark and select "Add Risk/Issue" from the menu.

To add a Risk or Issue to a Minimum Parameter, select an answer from the drop-down menu for each Minimum Parameter. To add additional Risks or Issues click the "Add Risk/Issue" button under the drop-down menu.

Criticality

Do these systems (Source, Consumer, or Transport Methodology) adequately support this Critical Information Need? Yes

Data sharing characteristics for each System Implementation are further defined here





Process Analysis: Risks and Issues



- Risks and Issues are generated based on a user's inputs in the System Implementation section

**Results from Architecture Analysis Using EISP Tool
Management of Information Dependency Risk and Issues**

Risk

Risk ID: Operational Risk 1
Risk Name:
Impacted Activity:
Source of Risk:
Risk Type:
Risk Level:
Likelihood:
Consequence:
Issue Level:
Risk Name:

Performance: Is there an impact to technical performance and to what level?
 Schedule: Is there an impact to schedule performance and to what level?
 Cost: Does the risk only impact lifecycle cost?

To add a new paragraph, right-click on the table and select "Add" from the pop-up menu. Click in the new row to add text. Each row in the table will appear as a formatted paragraph in the final output.

Depth and	1	2	3	4	5
5	Green	Yellow	Red	Red	Red
4	Green	Yellow	Yellow	Red	Red
3	Green	Green	Yellow	Yellow	Yellow
2	Green	Green	Green	Green	Yellow
1	Green	Green	Green	Green	Green

Consequence

2025 RELEASE UNDER E.O. 14176

To add a new paragraph, right-click on the table and select "Add" from the pop-up menu. Click in the new row to add text. Each row in the table will appear as a formatted paragraph in the final output.

Mitigation Strategy

OK Cancel

Accuracy of +/- .5 NM.

To add a new paragraph, right-click on the table and select "Add" from the pop-up menu. Click in the new row to add text. Each row in the table will appear as a formatted paragraph in the final output.

relying on this platform at risk.



Utilizing ISP Data



- ISP data is used to inform the ASD(NII)/DoD CIO position in key acquisition decision making processes as it:
 - Identifies programmatic interoperability and supportability risks and issues
 - Details compliance to the Net-Ready KPP through in depth analysis of integrated architecture, DoD IEA, Data and Services Strategy, IA Strategy, and Spectrum Supportability
- The ISP, along with the IA Strategy and Clinger-Cohen Act compliance, is rolled into a DoD CIO position in decision meetings.
 - PMs brief any interoperability issues and/or risks that are generated as a result of the EISP process
- ISPs can identify interoperability and information integration issues within programs at an early stage in the development lifecycle
- Because it is one of the few design documents at MS B, ISP data is leveraged by Systems Engineering validations early in a program's lifecycle
- ISPs are used by the Testing community to confirm requirements with system functions



Automatic Imports with the EISP Web Application



- The EISP Enterprise Service will automatically import architecture information, reducing the burden on the PM to manually enter data into the tool
- DoDAF 2.0 products that are created in accordance with the DoDAF Meta Model (DM2) Physical Exchange Specification (PES) can be automatically imported into the web application to populate the Process Analysis section of the tool
- The EISP will also be able to import architecture products developed using tools that adhere to the Unified Profile for DoDAF/MODAF (UPDM)
 - The UPDM is being adopted by tool vendors as a standard for exporting architecture data
 - UPDM Version 1.0 was officially published by OMG Finalization 26 Jun 09
 - UPDM is moving to also become an International Standardization at ISO
 - DoD has approved UPDM In DISR as a Emerging Standard
 - DoD and MOD Strongly Supports Industry Standardization of UPDM



EISP Enterprise Service Version



EISP is transitioning to a web service which will:

- Codify DoD CIO Interoperability policy in an Enterprise Solution that is available across the DoD to:
 - provide a more effective and efficient process for Program Managers to identify Interoperability risks and issues
 - Provide transparency to the data required for specific interoperability policy oversight and monitoring and makes it available to those organizations that can use it for other analytical purposes
- Allow automatic data import from authoritative data repositories increasing accuracy of data (e.g. GTG, DITPR, DARS)
- Expose data resulting from architectural analysis so that it is accessible and discoverable to allow deep dive cross-program reviews
- Provide a collaborative environment to capture, store, search, and reuse the data resulting from architectural analysis

We have partnered with DISA to rapidly field this web capability, leveraging DISA's common development environment and existing web framework, and to host the EISP on the DISA RACE

This web service is being developed in accordance with the Enterprise Service Designation process to ensure compliance with the policy and to help to formalize the process for future programs



What's Next



- EISP Enterprise Service Version completed 2010
- Sharing authoritative data across organizational boundaries:
 - DISA
 - AT&L
 - JS J6
 - JS J8
 - JFCOM J8
- Automated Analytical Outputs
 - Additional XML scripts
 - Visualizations
- Future Improvements
 - Web 2.0 capabilities
 - Real-time Collaboration



For more information, please contact:

Mr. Ed Zick

DoD CIO (SP&IM)

Edward.Zick@osd.mil

(703) 601-4729 x115

Mr. Bob Hayes

DoD CIO (SP&IM)

Bob.Hayes@osd.mil

(703) 601-4729 X155

Download Version 2.0 of the EISP at:

<https://jcpat.csd.disa.mil>