Information Support Plan (ISP) Tailored Information Support Plan (TISP)

Information Exchange Forum
Session: 5 and 6
HQDA CIO/G-6

Jacqueline Zachgo
Interoperability & Certification Division

KEY PLAYERS
DoD/J8 – ISP/TISP I&S Certification Authority
HQDA CIO/G-6 – Army ISP /TISP Approval Authority
AONS/AOJ – Facilitates ISP/TISP approval/production/adjudication
PEOS/PMS/MATDEVS – Develops ISP/TISP
FaNS/JITC – Use I&S certified ISP for development of test threads & interoperability certification testing
ISP Relationship Between DOD Acquisition, JCIDS, & the I&S Certification Process
Purpose of the ISP/TISP
Tailored ISP (TISP)
Approval for Entry into TISP Program
Core ISP Components
Army Required ISP/TISP DoDAF Views
Army Utilization of the ISP/TISP
Army ISP Review & Approval Process
HQDA CIO/G-6 ISP/TISP Review Process (MS C)
Legacy ISP Waivers
System of System (SOS) ISPs
Change Pages & Updated ISPs
Key ISP/TISP Take-A-Ways
AONS ISP POCs
Governing Documentation
Relationship Between the DOD Acquisition, JCIDS, and I&S Certification Process

DOD 5000
- Pre-Systems Acquisition
  - Initial Capability Document (ICD)
  - DOT&E Review
- Systems Acquisition
  - Capability Development Document (CDD)
  - JS J-6 I&S Cert
- Production & Development
  - Capability Production Document (CPD)
  - JS J-6 I&S Cert
- Operations & Support
  - Svc/Agency Op Testing
  - DISA (JITC) T&E Cert

Program Milestones

ISP Process DOD 4630
- Initial ISP
- Incremental ISP Annex
- Revised ISP
- ISP of Record
- Updated ISP

Space Program Milestones
- Initial ISP
- Revised ISP
- ISP of Record
- Updated ISP

Ref: CJCSI 6212.01E
Purpose of ISP/TISP

An ISP/TISP is:

• Required for all IT & NSS systems unless they have been granted OSD approval for an ISP waiver/exemption

• A DoD tool to synchronize, document and resolve interoperability issues between supported and supporting programs during the development stage

• Illustration of how the system and technical implementation meets the needs of the User

• The first time a program’s technical aspects are depicted and interrelationships with other systems/applications are technically defined

• Insures a design to fully integrate solutions that account for horizontal and vertical interactions
Tailored ISP (TISP)

★ A TISP is:

• An abbreviated version of the ISP
• Fewer architectural products and analysis requirements
• Only ACAT II and below programs which are NOT on the Special interest list are eligible to request entry into the TISP Program

★ All systems must obtain Joint Staff approval for entry into the TISP Program

★ All ISP/TISPs must receive Joint Staff Interoperability and Sustainability (I&S) Certification
Approval for Entry into TISP Program

- PM contacts HQDA, CIO/G-6, AONS, AOJ POC to determine System eligibility, evaluation, and guidance on the TISP process
- PM completes required documentation and forwards to HQDA CIO/G-6, AONS AOJ, Army Interoperability Certification Panel (ICP) Representative
- Army ICP Representative submits the request to Joint Staff (JS) for review and action
- If the request is approved, the PM receives a JS approval memo that identifies a TISP delivery date and any JS guidance
- If the request is not approved, the PM will be required to develop an ISP
- PM develops TISP and submit to AONS AOJ ISP team for review and entry into the formal ISP/TISP staffing process
Core ISP/TISP Components

★ Introduction
  • High-level programmatic information
  • Program Status

★ Analysis
  • Development of DoDAF products (Architectural Views)
  • Analysis of interrelationships with supported(ing) programs
  • NR-KPP (Five Elements)
    ▪ Compliant Solution Architectures, Data and Service Strategies, GIG Technical Guidance (GTG), Information Assurance (IA), and Supportability Requirements

★ Issues
  • Operational/Technical Issues
  • Resolution Path for resolving Issues
<table>
<thead>
<tr>
<th>Name</th>
<th>ISP</th>
<th>TISP*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview &amp; Summary Information</td>
<td>AV-1</td>
<td>AV-1</td>
</tr>
<tr>
<td>High-Level Operational Concept Graphic</td>
<td>OV-1</td>
<td>OV-1</td>
</tr>
<tr>
<td>Operational Node Connectivity Description</td>
<td>OV-2</td>
<td>N/A</td>
</tr>
<tr>
<td>Operational Information Exchange Matrix</td>
<td>OV-3</td>
<td>OV-3</td>
</tr>
<tr>
<td>Organizational Relationships Chart</td>
<td>OV-4</td>
<td>N/A</td>
</tr>
<tr>
<td>Operational Activity Model</td>
<td>OV-5</td>
<td>OV-5</td>
</tr>
<tr>
<td>Operational Event-Trace Description</td>
<td>OV-6C</td>
<td>OV-6c</td>
</tr>
<tr>
<td>Logical Data Model</td>
<td>OV-7</td>
<td>N/A</td>
</tr>
<tr>
<td>Systems Interface Description</td>
<td>N/A</td>
<td>SV-1</td>
</tr>
<tr>
<td>Systems Communication Description</td>
<td>SV-2</td>
<td>N/A</td>
</tr>
<tr>
<td>Systems Functionality Description</td>
<td>SV-4</td>
<td>N/A</td>
</tr>
<tr>
<td>Operational Activity to Systems Function Traceability Matrix</td>
<td>SV-5</td>
<td>SV-5</td>
</tr>
<tr>
<td>Systems Data Exchange Matrix</td>
<td>SV-6</td>
<td>SV-6</td>
</tr>
<tr>
<td>Systems-Event-Trace Description</td>
<td>SV-10c</td>
<td>SV-10c</td>
</tr>
<tr>
<td>Physical Schema</td>
<td>SV-11</td>
<td>N/A</td>
</tr>
<tr>
<td>Technical Standards Profile</td>
<td>TV-1</td>
<td>TV-1</td>
</tr>
<tr>
<td>Technical Standards Forecast</td>
<td>TV-2</td>
<td>N/A</td>
</tr>
</tbody>
</table>

*PM must apply to HQDA/J8I/OSD (NII) for approval to produce a TISP*
Armý Utilization of the ISP

★ A way to ensure that interoperability and supportability are addressed throughout a program’s life-cycle -- the ISP is a living document.

★ Documents current & future interoperability through analysis of the integrated architectures.

★ Supports test-thread development for the conduct of Army Interoperability Certification (AIC) & JITC testing – ISP is Entrance Criteria.

★ Used to establish interoperability capabilities which are used in AIC/JITC testing.
Army ISP Review Process

Staffing Process Repeated at MS B, CDR, MS C LRIP & ISP Update (If Required)
ISP/TISP's Submitted for Official Review NLT 3 Months Prior to MS B, CDR & MS C LRIP & NLT 6 Months In Support of AIC Testing

- PM
  - Update/Develop ISP
  - Conduct Internal/External PEO ISP Review

- PM
  - Coordinate DoD, Joint, & Army Review

- 30 Days
  - CIO/G-6

- 2 Weeks
  - CIO/G-6

- 90 Days
  - PM

- 10 Days
  - J8

- 90 Days
  - PM

- 21 Days
  - J8

- 12-14 Days
  - G-6/J8

- Army Approval/ Joint Supportability Certification
  - **ISP uploaded to JCPAT by AOJ for OASD/J8I ONLY AFTER CIO/G-6 Approval

1. ISP w/ PEO Cover Letter to CIO/G-6 AOJ
2. J8
3. PM
4. J8

Final or Updated ISP reviewed by J8 as Stage II review. If no critical comments then I&S Certification granted by J8.
PM adjudicates comments and submits revised ISP back for Final Stage II J8 review
Initial, Final or Updated ISP reviewed by J8 as Stage I review

MS B,C & ISP Update Only
HQDA CIO/G-6 ISP/TISP Review Process (MS C)

- HQDA CIO/G-6 AONS AOJ AO checks the ISP for content/quality prior to distribution for Army/DoD review
- Signatory authority for ISP tasking memo has been delegated to the Director of System-of-System (SoS)/Joint Interoperability Certification
- Army and/or Joint Services have 30 days to review and comment on the ISP/TISP
- PM must adjudicate ALL comments (critical, substantive, administrative) and AOJ verifies comments have been adjudicated
- HQDA CIO/G-6 AONS AOJ AO develops the approval packet for signature: the Director of Interoperability & Certification; the Deputy Director of AONS; XO for the HQDA CIO/G-6; and the HQDA CIO/G-6
- If approved, HQDA CIO/G-6 AONS AOJ AO loads the ISP/TISP into the Joint C4I Program Assessment Tool (JCPAT) which initiates the J8 Review
- Upon successfully completion of the J8 review, the ISP/TISP will receive JS Interoperability & Supportability Certification (I&S Cert)
Programs may apply for Legacy ISP Waiver if:

- No future modifications/upgrades planned
- No R&D/procurement funds remaining and/or:
  - Fixed retirement date (within 5 years)
- Proven interoperability track record for years
- JCIDS documentation is waived by the JS and the program lacks updated requirement documentation
- Positive post-AIC/JITC assessments
- PM contacts HQDA CIO/G-6 ISP POC to discuss criteria that must be met to receive approval of a Waiver. ISP POC emails the PM the application. PM submits completed application to the ISP POC who reviews and submits to ICP Rep for formal submission to J8.
When practical, development of SoS ISPs are encouraged

SoS ISPs can be utilized if a lot of common architectural information can be shared

The main body of the ISP will contain the common information while system specific information will be discussed in separate annexes

Saves money and review/approval time

Avoids development of redundant architectures and analysis
If a system has changed since its approval (capabilities, interfaces, software, versions, etc.) then a change page and/or an updated ISP is required.

Once an ISP has received an I&S certification, change pages may be submitted to document minor changes that did not effect the capabilities or layout of the system. The change pages will be submitted to HQDA CIO/G-6 AONS, AOJ ISP AO for review and Army approval. Once approved the change pages may be turned in to reflect the current state of a system to satisfy interoperability testing entrance criteria.

If the changes are very extensive or numerous, the document may be required to submit an Updated ISP/TISP and undergo a review. If an Updated ISP is required a submittal memo must be sent along with the ISP to HQDA CIO/G-6 to initiate the review. The ISP will be reviewed by OASD and J8 and an I&S approval memo will be reissued for the updated ISP.
Key ISP/TISP Take-A-Ways

- Required for all IT & NSS systems unless they have been granted OSD approval for an ISP waiver/exemption

- A system must obtain Joint Staff approval for entry into the TISP Program

- All ISP/TISPs must receive Joint Staff Interoperability and Sustainability (I&S) Certification

- Effective 1 Jan 2011, Army directed all ISP/TISPs be developed using the Enhanced Information Support Plan (EISP) tool
Army AONS AOJ ISP POCs:

Mrs. Jacqueline Zachgo, Branch Chief, 703-545-2583
jacqueline.d.zachgo.civ@mail.mil

Mr. Jim Bronson, 703-545-1428
james.l.bronson1.ctr@mail.mil

Mr. Ken Dunbar, 703-545-1421
keneth.w.dunbar.ctr@mail.mil
Governing Documentation

DoD Net-Centric Data Strategy, 09 May 2003
DoDD 5000.1, The Defense Acquisition System, 12 May 03
DoD Architecture Framework v1.5, 23 April 2007
CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems, 15 Dec 08
JROCM, 236-03, Policy for Updating Capabilities Documents to Incorporate the Net Ready Key Performance Parameter (NR-KPP), 19 Dec 03
AR 70-1, Army Acquisition Policy, 31 Dec 03
CJCSI 3170.01D, Joint Capabilities Integration and Development Systems, 12 Mar 04
DoD Directive 4630.5, Interoperability and Supportability of IT and NSS, 05 May 04
CJCSI 3312.01, Joint Military Intelligence Requirements Certification, 10 May 04
DoD Instruction 4630.8 Procedures for Interoperability and Supportability of IT and NSS, 30 Jun 04
DoDI 8320.2, Data Sharing in a Net-Centric DoD, 02 Dec 04
National Security Space Acquisition Policy 03-01, 27 Dec 04
Net-Centric Checklist, v 2.1.4, OSD(NII)
DAU Acquisition Guidebook
Joint Interoperability Test Certification Governance and Process Evolution

CAPT Ron Greiff
Joint Staff, J8, Interoperability Certification Panel
703-545-2546
ronald.greiff@js.pentagon.mil
★ Governance
★ Who’s Who
★ Requirement
★ Process
★ MCEB Panels
★ Future
  • CJCSI 6212.01F and Refined NR KPP
  • 804
  • Rapid Acquisition
  • Agile strategies
DODD 4630.5
IT/NSS Interoperability shall be verified early, and with sufficient frequency throughout a system’s life.

DODD 5105.19
DISA shall ensure end-to-end interoperability.

CJCSI 6212.01
All IT/NSS must be evaluated and certified for Joint Interoperability by DISA (JITC).

DOD 4630/5000
Interoperability is the ability to provide and accept data, information, material and services... includes both the tech exchange of info and the end to end operational effectiveness of that exchange, as required for mission accomplishment.

DOD 4630.8
All IT/NSS... must be tested for interoperability before fielding.... And certified by DISA (JITC).

CJCSI 3170.01
Establishes JCIDS w/NR-KPP for CRD, CDD and CPD.

DOD 5000 series
For IT/NSS...JITC shall provide system interop test cert memoranda... Throughout system life-cycle regardless of ACAT.
Who's Who in Interoperability

★ DOD CIO
★ Joint Staff
★ JITC
★ Services
★ Agency’s
All IT and NSS, regardless of ACAT, must be tested for interoperability before fielding and the test results evaluated and systems certified by the DISA (JITC).

IT and NSS interoperability test and evaluation shall be conducted throughout a system's life, and should be achieved as early as is practical to support scheduled acquisition or procurement decisions.

Interoperability testing may be performed in conjunction with other testing (i.e., DT&E, OT&E, early-user test) whenever possible to conserve resources.
Interoperability Test Certification Process

Step 1: Identify & Verify Requirements
- CPD
- ISP
- TISP
- NR-KPP
- Package
- ISP Annex
- UCR

Step 2: Develop Certification Evaluation Approach
- ICEP/ITP Development

Step 3: Collect & Analyze Interoperability Data
- Developmental Test
- Standards Conformance
- Operational Test
- Exercise Data
- Interoperability Test

Step 4: Determine the Interoperability Status
- Certify
  - Standards Conformance
  - Interoperability Assessment
  - OTRR Interoperability Statement
  - Special Interoperability
    - Limited Joint IOP Test Certification
    - Interim Joint IOP Test Certification
    - Joint Interoperability Test Certification

Any changes that may affect Interoperability

Joint Staff

PM/PEO

Users

JITC

Testers

Recertification

4 years

1 Evaluations for Special certifications are performed against the JS-approved Unified Capabilities Requirements (UCR) documents
Joint Staff chairs two panels under the Military Communications-Electronics Board (MCEB)

- Interoperability Certification Panel (ICP)--grants Interim Certificates to Operate (ICTO) for systems in the Interoperability test Process.

- Interoperability Panel (IP)--IP provides forum for improvement of the interoperability process.
Promote, enhance, and maintain compatibility and interoperability of IT/NSS systems

Accomplish through a formal process for identifying and resolving critical IT/NSS interoperability testing policy and testing issues

Subordinate to the 3-star Military Communications-Electronics Board (MCEB)

Chaired by Joint Staff, DISA/JITC is Executive Agent

Chartered-Members: Services, DISA, NSA, DIA, COCOMs

Non-chartered members: DOT&E, USD(AT&L), ASD(NII)

DOD CIO
ICP Process Improvements

★ Interoperability Certification Panel over the years has modified its processes:

- Tailored Information Support Plan (TISP): Focused on Non ACAT, Current/Legacy systems, rapid acquisitions

- Information Support Plan (ISP) Legacy program: Waives ISPs and testing for systems/programs with no R&D funding, follow-on systems in development or near fielded, being replaced/retired within 5 years, no interoperability issues

- Interoperability Test exemptions: Waives testing for systems w/ no interoperability deficiencies, limited joint interfaces, and recommended by JITC
Interim Certificate to Operate (ICTOs) grant a temporary reprieve to allow fielded systems to obtain full certification.

Any non-certified operational system that touches the GIG requires an ICTO if not fully certified.

Requests made through the ICP Representatives.
Provides oversight of C4 Interoperability, focusing on policy and procedural issues to include:

- DOD interoperability guidance/directives, architectures, technical, operational and procedural standards, and data standardization
- DOD positions on interoperability issues that affect joint, combined, coalition and interagency operations

Chaired by Joint Staff

Members: Service representatives, DISA, NSA, DIA, COCOMs
Future

★ CJCSI 6212.01 F and Refined NR KPP
★ 804
★ Rapid Acquisition
★ Agile strategies
## NR KPP

**Attributes**

<table>
<thead>
<tr>
<th>SPT MIL OPS</th>
<th>Threshold</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mission:</strong> Ballistic Missile Defense</td>
<td><strong>Measure:</strong> Minutes warning provided</td>
<td><strong>Threshold:</strong> 10 min</td>
</tr>
<tr>
<td><strong>Measure:</strong> Percent of incoming missiles destroyed</td>
<td><strong>Objective:</strong> 2 incoming missiles</td>
<td></td>
</tr>
<tr>
<td><strong>Conditions:</strong> Number of incoming missiles</td>
<td><strong>Satisfy Technical Requirements</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Mission Activities:** Detect Contacts

| **Measure:** Minutes to recognize contacts | **Conditions:** Contact Speed |

**ENTER/MANAGED IN NET**

<table>
<thead>
<tr>
<th>Network: SIPRNET</th>
<th><strong>Measure:</strong> Time to connect to an operational network from power up</th>
<th><strong>Conditions:</strong> Threats to the network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threshold:</strong> 2 min</td>
<td><strong>Objective:</strong> During a Denial of Service attack on the network</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network: NIPRNET</th>
<th><strong>Measure:</strong> Time to connect to an operational network from power up</th>
<th><strong>Conditions:</strong> Threats to the network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threshold:</strong> 2 min</td>
<td><strong>Objective:</strong> Doesn't support a joint critical activity</td>
<td></td>
</tr>
</tbody>
</table>

**EXCHANGE INFORMATION**

<table>
<thead>
<tr>
<th>Information Element: Target Data</th>
<th><strong>Measure:</strong> Time to failover to backup server</th>
<th><strong>Conditions:</strong> Availability of NOC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Measure:</strong> Time to recover from a close access attack on the server</td>
<td><strong>Threshold:</strong> 10 sec</td>
<td><strong>Objective:</strong> 10 sec</td>
</tr>
<tr>
<td><strong>Measure:</strong> Latency of data</td>
<td><strong>Threshold:</strong> 3 minutes</td>
<td><strong>Objective:</strong> 5 minutes</td>
</tr>
<tr>
<td><strong>Measure:</strong> Strength of encryption</td>
<td><strong>Threshold:</strong> 2 minutes</td>
<td><strong>Objective:</strong> 2 minutes</td>
</tr>
<tr>
<td><strong>Conditions:</strong> NSA Certified Type 1 NSA Certified Type 1</td>
<td><strong>NOC unavailable</strong></td>
<td><strong>NOC unavailable</strong></td>
</tr>
</tbody>
</table>

**NR KPP**

- **See example to the right**
- **And NR KPP Architecture**
- **And DD Form 1494, Bandwidth and Spectrum Analysis**

*Measurable and testable NR KPP. Threshold and Objective values developed by PM through use of Architecture*
## NR KPP Process

<table>
<thead>
<tr>
<th>NR-KPP Development Step</th>
<th>NR-KPP Attribute</th>
<th>Attribute Details</th>
<th>Measures</th>
<th>Sample Data Sources</th>
<th>NR-KPP MOE or MOP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission Analysis</td>
<td>Support to Military Operations Support to Military Operations</td>
<td>Military Operation (e.g., mission areas or mission threads)</td>
<td>MOEs used to determine the success of the military operation</td>
<td>JMETL, JMT, UJTL, and METL</td>
<td>MOE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operational tasks required by the military operations</td>
<td>Conditions under which the military operations must be executed</td>
<td>JMETL, JMT, UJTL, and METL</td>
<td>MOP</td>
</tr>
<tr>
<td>Information Analysis</td>
<td>Entered and managed on the network</td>
<td>Which networks do the net-centric military operations require</td>
<td>MOP for entering the network</td>
<td>N/A</td>
<td>MOP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information produced and consumed by each military operation and operational task</td>
<td>MOP for management in the network</td>
<td>N/A</td>
<td>MOP</td>
</tr>
<tr>
<td></td>
<td>Effectively exchanges information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems Engineering and Architecture</td>
<td>Supports all 3 attributes</td>
<td>Ensures that IT satisfies the attribute requirements</td>
<td>Provides traceability from the IT MOPs to the derived operational requirements</td>
<td>OVs and SVs</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Translating a Table from a Document

### Support Net-Centric Military Operations

<table>
<thead>
<tr>
<th>NR-KPP Attribute</th>
<th>Key Performance Parameter</th>
<th>Threshold</th>
<th>Objective</th>
</tr>
</thead>
</table>
| Mission: Tracking and locating (Finding, Fixing, Finishing) High-Value Target (HVT) | - Measure: Timely, actionable dissemination of acquisition data for HVT  
- Conditions: Targeting - quality data to the neutralizing/tracking entity | --10 minutes | -- Near-Real-Time  
-- Area denial of HVT activities | -- HVT tracked, neutralized |
| Mission Activities: Find HVT | -- Measure: Location accuracy  
-- Conditions: Individual differentiation | -- 100 Meter circle | -- 25 Meter circle  
-- Identify armed/not armed | -- Identify individual |

### Enter and Be Managed in the Network

<table>
<thead>
<tr>
<th>NR-KPP Attribute</th>
<th>Key Performance Parameter</th>
<th>Threshold</th>
<th>Objective</th>
</tr>
</thead>
</table>
| Network: SIPRNET | -- Measure: Time to connect to an operational network from power up  
-- Conditions: Network connectivity | -- 2 minutes | -- 1 minute  
-- 99.8 | -- 99.9 |
| Network: NIPRNET | -- Measure: Time to connect to an operational network from power up  
-- Conditions: Network connectivity | -- 2 minutes | -- 1 minute  
-- 99.8 | -- 99.9 |

### Exchange Information

<table>
<thead>
<tr>
<th>NR-KPP Attribute</th>
<th>Key Performance Parameter</th>
<th>Threshold</th>
<th>Objective</th>
</tr>
</thead>
</table>
| Information Element: Target Data | -- Measure: Dissemination of HVT biographic and physical data  
-- Measure: Receipt of HVT data  
-- Measure: Latency of data  
-- Measure: Strength of encryption  
-- Conditions: Tactical/Geopolitical | -- 10 seconds  
-- LOS  
-- 5 seconds  
-- NSA certified type 1  
-- Permissive environment | -- 5 seconds  
-- BLOS  
-- 2 seconds  
-- NSA certified type 1  
-- Non-permissive environment |
### Architectural Data per CJCSI 6212.01F

<table>
<thead>
<tr>
<th></th>
<th>AV-1</th>
<th>AV-2</th>
<th>CV-2</th>
<th>CV-3</th>
<th>CV-5</th>
<th>CV-6</th>
<th>DIV-2 (OV-7)</th>
<th>DIV-3 (SV-11)</th>
<th>OV-1</th>
<th>OV-2</th>
<th>OV-3</th>
<th>OV-4</th>
<th>OV-5a</th>
<th>OV-5b</th>
<th>OV-6C</th>
<th>SV-1 or SvcV-1</th>
<th>SV-2 or SvcV-2</th>
<th>SV-4 or SvcV-4</th>
<th>SV-5 or SvcV-5</th>
<th>SV-6 or SvcV-6</th>
<th>StdV-1 (TV-1)</th>
<th>StdV-2 (TV-2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICD</td>
<td>2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDD</td>
<td>2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPD</td>
<td>2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1</td>
<td>1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>ISP</td>
<td>2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1</td>
<td>4</td>
<td>1,4</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>TISP</td>
<td>2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>1</td>
<td>1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

**Legend**
- X - Required
- O - Optional

**Note 1**
- Required only when IT and NSS collects, processes, or uses any shared data or when IT and NSS exposes, consumes or implements shared services.

**Note 2**
- The AV-1 must be registered, and must be public and released at the lowest classification level possible in DARS for compliance.

**Note 3**
- The technical portion of the StdV-1 and StdV-2 are built using DISRonline and must be current for compliance.

**Note 4**
- Not required for JROC approved Operational Requirements Documents.

---

X - Indicates new requirement in draft CJCSI 6212.01F and naming convention in the latest version of DODAF
Laurie Ann White, CISSP
Joint Staff, J8 Joint Testing Branch RM 1E1029
(703) 692-3801 DSN 222-3801
NIPR: laurie.white@js.pentagon.mil
SIPR: laurie.white@js.smil.mil

Charles Thornburg
Joint Staff, J8 Enterprise Architect RM 1E1029
(703) 692-0143 DSN 222-0143
NIPR: charles.thornburg@js.pentagon.mil
SIPR: charles.thornburg@js.smil.mil
Joint Interoperability Certification Opportunities

Mr. Mathew Meverden
DISA LNO
Phone: 254-532-8321, ext. 2024
Email: Mathew.Meverden@us.army.mil
Purpose:

• Inform attendees of additional opportunities for Army Systems to satisfy Joint Interoperability Certification Requirements
Events Focuses:

- Current Joint wartime mission challenges and gaps
- System of Systems Joint Architecture and Associated Standards
- System of Systems Joint Mission Thread Approach
- Relationship with USAF, Navy and Marines
- Event driven Joint Scenario that provides an opportunity for reciprocity of data for certification of multiple systems with one test event
- Utilize Joint Simulation/Stimulation and Data Collection and Analysis Tools
- 90% of US Army C4I systems and technical support expertise during AGILE Fire events was provided by CTSF staff
Joint Events Supported by US Army

- **AGILE Fire** - Supporting Air/Ground Integrated Layer Exploration (AGILE) Fire Joint Air Ground Integration

- **JAGIC** - Army provides Army Division and Brigade Tactical Operations Centers architectures at the CTSF and ADAMS Cell joined by two Air Force systems, Tactical Air Control Party-Close Air Support System (TACP-CASS), and Theater Battle Command Management System (TBMCS) - creating what's known as the Joint Air Ground Integration Cell (JAGIC)

- **JMECS-NS** - Joint Master Scenario Events List Exercise Control Station-No Simulation (JMECS-NS) Software Version 3.5, Software Block 2 (SWB2), Engineering Assessment – JFCOM sponsored event

- Above utilize CTSF Resources
Other Joint Events Supported by US Army

- **Joint Data Integration (JDI)** Land Data Management Tactics, Techniques and Procedures (TTP) Verification Event (SWB2) – OSD Joint Test and Evaluation (JT&E) Office sponsored event. (Common Operational Picture (COP) Management)

- **Deployable Joint Command and Control (DJC2)** Interoperability Test with US Army LandWarNet/BC (ABCS) systems (SWB2) – AFRICOM sponsored event

- **C4ISR On-The-Move (OTM)** Event, Fort Dix, New Jersey – PM C4ISR-OTM sponsored event to experiment with new Joint technologies for the future force

- **Coalition Attack Guidance Experiment (CAGE)** – originally hosted by the Canadian Forces Warfighting Centre (CFWC) Joint Fires Support Battle Lab to analyze evolving Coalition C2 configuration intended for ISAF – CAGE Working Group requesting CTSF support because of its interoperability and network expertise

- **Joint Users Interoperability Communications Exercise (JUICE)** focus on technologies which provide improvements to existing operational capabilities and fill operational gaps to maintain and sustain a light agile and lethal fighting force
DOD Interoperability Communications Exercise (DICE) - DoD exercise whose principal purpose is to generate system-level, joint interoperability assessments and certifications to support the fielding of interoperable systems to the warfighter – run by the Joint Interoperability Test Command (JITC)

Empire Challenge (EC) - annual Intelligence, Surveillance and Reconnaissance (ISR) focused on providing critical intelligence to the warfighter with its primary location in Fort Huachuca, AZ sponsored by the Office of the USD, Intelligence

Unified Endeavor (UE) – A simulation-driven Computer Aided Exercise (CAX) for Joint Task Force Component Commanders to train at the operational level – hosted by USJFCOM

Plus Others
AGILE Fire Working Group

★ Purpose: Responsible for planning, coordinating, executing and reporting outcome of AGILE Fire events

★ Authority: Endorsed by US Army CIO/G-6 and USAF ACC and USAF SIMAF, US Navy (China Lake), Marine Corps (MCTSSA) and, PM-JUDIE

★ Management: Co-chaired by US Army CTSF Technical Director and USAF ACC and USAF SIMAF Technical Directors

★ Duties: Coordinates AGILE Fire events per US Army TRADOC and USAF ACC direction
  • Provides results/recommendations on Joint Fires operational mission TTPs for current and future fight
  • Works with capability owners on limitations discovered
AGILE Fire has become the “go to” event for conducting Joint Fires SoS integration and interoperability and Joint Fires TTP validation and/or development

Effectiveness and Efficiencies:
- Joint Mission Thread-focused
- Joint Current and Future Fight Focused

Delivery:
- Make what we have ....Work....
- Operational Focused

Influence:
- Joint Missions driving the process (soon to include Coalition influence)
- Maintaining interoperability

People:
- Right People/Right Skills/Right Place – knowledge, skill sets, and execution
Program Managers from all services use data to enhance and fix System-of-System (SoS) interoperability

Dynamic Air Space Management (DASM) prototype exceeded expectations
- M2M exchange showing real-time exchange of Airspace Control Measures

Joint Air Ground Integration Cell (JAGIC)
- Refinement and validation of airspace management TTPs
- TTPs developed to date to be deployed in near future

TACP-CASS – AFATDS
- Integration and interoperability issues identified in Phase II; provided to PMs
- Execution in Phase III expected to show capability ready for certification

JITC Provides Oversight and Collects Data for Joint Certification Purposes

FOS/PFED
- Added JMETC/SDREN capability to the Fires Software Engineering Division (FSED) facility
- Ft Sill’s ability to participate expected to decrease capability development time

NEW/SDB II
- Mature J11 message set
- Develop, exercise, and mature Tactics, Techniques, and Procedures

LVC Verification, Validation and Accreditation
- OSD funded effort to provide a consistent way to identify and present risk areas to customer
- Initial customer feedback very positive on the structured 5 step process
Joint & Coalition Integration

AGILE FIRE
Close Air Support
(AFTADS communications path, w/NEW weapon)

CFBLNet

CTE2
Coalition Test & Evaluation Environment – Representative of AMN

Current Planned

IBCT
TOC/FSE (RTC)

JFACC/JAOC (Langley)

CRC (Eglin)

JTAC/JFO (Eglin)

F-15 LCS (Eglin)

JAGIC
Senior FSE/AJAC (Ft Hood)

SBCT
TOC/FSE (WSMR)

AMN

2011-08-24 // Joint Interoperability Certification Opportunities
Questions?

Mr. Mathew Meverden  
DISA LNO  
Phone: 254-532-8321, ext. 2024  
Email: Mathew.Meverden@us.army.mil
USCENTCOM Regulation (CCR) 25-200, Information Resources Management (IRM)

Information Exchange Forum
Session: 5
HQDA CIO/G-6

Mr. Brad Hanna
CIO Support Branch (CCJ6-PI)
CENTCOM J6 Programs and Architectures Division
Why CCR 25-200 (IRM)?

AOR requested help…

- Protect the network…
  while enabling capabilities

- Manage AOR network capabilities
  NOW & FUTURE

- Persistent force rotations, each with “critical” systems

- Ease the AOR integration burden

...AND...

- Accounting for and managing IT as portfolios
  is law, policy and good practice
Effectively Enable AOR Capabilities in a Deliberate, Coordinated Manner
Two sides of the IRM brain...

25-200 HQ Process
Requirements to enable HQ capabilities (Tampa and Forward):
- Chapter 4 and Appendix C/D
- Change Request, Quad Chart, 3215
- Directorate Approval
- Technical Analysis
- Functional Analysis
- Final approval authority by cost

25-200 AOR Process
Requirements to introduce/enable capabilities in CENTCOM AOR
- Chapter 5 and Appendix E/F
- J6 CIO Support Branch
- AOR 25-200 Packet
- Technical Analysis
- Functional Analysis
- CIO approves “introduction”
- DAA approves connection/testing/operation

Common thread is Portfolio Management (PfM)
- Chapter 3
- Weaved into all other chapters
- Leveraged to ensure decisions result in the best mix of capabilities to support mission needs and minimize issues, gaps and overlaps.

<table>
<thead>
<tr>
<th>Joint Capability Area (JCA) Portfolio</th>
<th>Lead Directorate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Support</td>
<td>CCJ1</td>
</tr>
<tr>
<td>Battlespace Awareness</td>
<td>CCJ2</td>
</tr>
<tr>
<td>Force Application</td>
<td>CCJ3</td>
</tr>
<tr>
<td>Command &amp; Control</td>
<td>CCJ3</td>
</tr>
<tr>
<td>Protection</td>
<td>CCJ3</td>
</tr>
<tr>
<td>Logistics</td>
<td>CCJ4</td>
</tr>
<tr>
<td>Building Partnerships</td>
<td>CCJ5</td>
</tr>
<tr>
<td>Net-Centric</td>
<td>CCJ6</td>
</tr>
<tr>
<td>Corporate Management &amp; Support</td>
<td>CCJ8</td>
</tr>
</tbody>
</table>
Where 25-200 Fits... CENTCOM AOR Battlespace Prep

CCR 25-200 AOR PROCESS

**Functional Analysis**
- Ensure valid CENTCOM requirement
- Establish management of theater capabilities within and across IT portfolios

**Technical Analysis**
Ensure capability minimums:
- Interoperability
- Information Assurance
- Sustainability

Submit AOR Packet *(template)*

CCR 25-206 NETOPS

CIO Approval To Introduce *(memo)*
Theater DAA Approval To Connect / Operate

For CX-I, not issued without Joint Staff & CCJ3 validation
AOR Packet:

1. Requesting organization information
2. System/application title
3. System/application description
4. “CENTCOM” GO/FO requirement validation
5. Expected installation/activation dates
6. Primary and secondary IT Portfolio
7. General system information
8. CONOPS or CONEMP
9. Security Accreditation Package (signed)—DIACAP/DCID
10. Joint Interoperability Certification (DISA/JITC)
11. Operational and/or evaluation tests
12. System Requirements (hardware/software, Power/HVAC)
13. Bandwidth/Transport Requirements (Port & Protocols)
14. Radio Frequency Requirements
15. COMSEC Requirements
16. Sustainment (initial/out-year plan)
17. Architectural Views (OV1, OV2, OV5, SV1, SV2, TV1)

CCR 25-200 requests items which are already required IAW DoD and Joint Staff Instructions/Directives

Information / artifacts required for processing

Items in Red are absolutes

Incomplete packet is the most common reason for delayed approval

Common misunderstanding
1. Requesting organization information
2. System/application title
3. System/application description
4. “CENTCOM” GO/FO requirement validation
5. Expected installation/activation dates
6. Primary and secondary IT Portfolio
7. General system information
8. CONOPS or CONEMP
9. Security Accreditation Package (signed)—DIACAP/DCID
10. Joint Interoperability Certification (DISA/JITC)
11. Operational and/or evaluation tests
12. System Requirements (hardware/software, Power/HVAC)
13. Bandwidth/Transport Requirements (Port & Protocols)
14. Radio Frequency Requirements
15. COMSEC Requirements
16. Sustainment (initial/out-year plan)
17. Architectural Views (OV1, OV2, OV5, SV1, SV2, TV1)

- Joint Pub 6-0
- CJCSI 3137.01D
- CJCSI 3137.01G
- CJCSI 6212.01D
- CJCSI 6212.01E
- CJCSI 6510.06A
- CJCSI 6510.01F
- CJCSM 6510.01
- DoDD 5230.11
- DoDD 5000.1
- DoDI 5000.02
- DoDI 7075.20
- DoDD 8000.01
- DoDI 815.01
- DoDI 8115.02
- EO 12958
- FRAGO 13 to JTF-GNO OPORD 05-01
- Joint CONOPS for GIG NETOPS
1. Requesting organization information
2. System/application title
3. System/application description
4. “CENTCOM” GO/FO requirement validation
5. Expected installation/activation dates
6. Primary and secondary IT Portfolio
7. General system information
8. CONOPS or CONEMP
9. Security Accreditation Package (signed)—DIACAP/DCID
10. Joint Interoperability Certification (DISA/JITC)
11. Operational and/or evaluation tests
12. System Requirements (hardware/software, Power/HVAC)
13. Bandwidth/Transport Requirements (Port & Protocols)
14. Radio Frequency Requirements
15. COMSEC Requirements
16. Sustainment (initial/out-year plan)
17. Architectural Views (OV1, OV2, OV5, SV1, SV2, TV1)
1. Requesting organization information
2. System/application title
3. System/application description
4. “CENTCOM” GO/FO requirement validation
5. Expected installation/activation dates
6. Primary and secondary IT Portfolio
7. General system information
8. CONOPS or CONEMP
9. Security Accreditation Package (signed)—DIACAP/DCID
10. Joint Interoperability Certification (DISA/JITC)
11. Operational and/or evaluation tests
12. System Requirements (hardware/software, Power/HVAC)
13. Bandwidth/Transport Requirements (Port & Protocols)
14. Radio Frequency Requirements
15. COMSEC Requirements
16. Sustainment (initial/out-year plan)
17. Architectural Views (OV1, OV2, OV5, SV1, SV2, TV1)

• DoDI 8500.2
• DoDI 8551.1
• CJCSI 3320.01B
• CJCSM 3320.01B
• CJCSI 6212.01E
• CJCSI 6510.06A
• CJCSI 6510.01F
• DoDI 5000.02
• Clinger-Cohen Act
• OMB A-130
• OMB A-11
• CJCSI 6212.01E
• DoDD 8000.01
• DoDD 5000.01
• DoDi 5000.02
• DoDi 4630.8
AOR IRM Portal


25-200 AOR Template > CCR 25-200

Does not address other processes for introduction of capabilities
Other Processes

🌟 25-200 is not the only CENTCOM process for introduction of capabilities to the AOR

🌟 Other processes include:

- CJCSI 6285 for MNIS (e.g., CX-I) (J3-C)
  - Deputy Division Chief, Steve Lesher (312-651-4149)
- DoDIIS / JWICS Operational Intelligence Requirements (J2-OS)
  - Systems Deputy Branch Chief, CDR Jeffery Johnson (312-651-0406)
- Information Exchange Requirements (IER) (J3-CM)
  - Information Management Branch Chief, Carlius Mapp (312-651-8865)
- Joint ISR Center (JISRC) (J3-O-ISR)
  - Reconnaissance and Space Deputy Branch Chief, Lt Col Keith Marlowe (312-651-8313)
- Cross Domain Solutions (CDS) (J6-CN)
  - CDS Specialist, Sandralea James, (312-651-6067)
- JUON or Services ONS (J8-ARC)
  - Lt Col Garrick Schroeder (312-651-4338)

🌟 TF 236 (Task L2-6-5) is aligning warfighter capability processes

Name change: 25-20, IAW new CENTCOM guidance

Reduce info/artifact requirements for:

- CENTCOM approved “urgent” needs (JUONS)
- CENTCOM GO/FO (AOR, J3, Portfolio Owner) validated request to “expedite” deployment - GO/FO accepts the risk
- “Minor version changes”; no CIO memo issued

Add coalition mission net requirements (6285, CIAV)

Continue evolution of IT Portfolio Mgmt

- Introduce IT Capability planning and IT Portfolio Owners
- Add info requirements tied to DITPR/SIPRNET IT Registry

Reflect org/process changes since last revision
Contacts

CMDR Steve Dryden, AUS
CENTCOM J6-PI
Chief, CIO Support Branch
DSN 312-651-3322

stephen.dryden.aus@centcom.mil
stephen.dryden.aus@centcom.smil.mil

CIOSPT@centcom.smil.mil

CMDR Steve Dryden, Mr. Brad Hanna, Mr. Anthony Leghart,
Mr. Jeff Terry, Mr. Dave Cadwell, Ms. Amanda Chiari,
Mr. Jerry Ingram, Mr. Mike Kopfer, Mr. Bill Lubliner