SUPPORT THE WARFIGHTER

DoD Statutory Responsibility

TITLE 10--ARMED FORCES

Sec. 2223. Information technology: additional responsibilities of Chief Information Officers

The DoD CIO shall:

Ensure the interoperability of information technology and national security systems throughout the Department of Defense
DoD CIO

Impetus for Change

- MOA between DoD CIO and JS (September 2011)
  - Transferred Interoperability Certification Panel (ICP) and Interoperability Panel (IP) to DoD CIO
  - Transferred responsibility for Interoperability Test and Certification to DoD CIO
  - Maintained JS role as certifier of the NR KPP

- CJCSI 6212.01F, Net Ready Key Performance Parameter (NR KPP), 21 March 2012
  - Reflects MOA changes in roles and responsibilities
  - Eliminates guidance for interoperability test and certification
  - Establishes procedures for the NR KPP certification

- DoD 4630.5/8 series, last issued in 2004, required update
DoD CIO

DoDD/I 4630 Interoperability Policy Issues

• No forcing function
• Interoperability governance structure outdated
• Previous JFCOM responsibilities unassigned
• USSTRATCOM/USCYBERCOM responsibilities not reflected
• Current Information Support Plan (ISP) process required update
DoDI 8330.01 Interoperability Approach

- Restricts policy to only interoperability – removes responsibilities and processes covered under separate policy (IA, standards, architecture)

- New division of roles and responsibilities:
  - Joint Staff responsible for the interoperability requirement (NR KPP)
  - DoD CIO responsible for interoperability test and certification, and interoperability governance

- Creates forcing function – interoperability test and certification a prerequisite for connection of IT, including NSS

- Streamlines the ISP process:
  - Re-establishes DoD Component as approval authority for the ISP
  - Removes details of ISP content from the policy – ISP format and content contained in the Defense Acquisition Guidebook, allowing more timely and responsive revision

- Establishes governance structure subordinate to the DoD CIO Executive Board

- Establishes JITC Interoperability Process Guide (IPG), containing processes and procedures for test, certification, and waiver requests
DoD CIO

Interoperability Policy Precepts

- IT that DoD Components use must interoperate with existing and planned systems (including applications) and equipment of joint, combined, and coalition forces, other U.S. Government departments and agencies, and non-governmental organizations.

- IT interoperability must be evaluated early and with sufficient frequency throughout a system’s life cycle to capture and assess changes affecting interoperability in a joint, multinational, and interagency environment.

- All IT, including defense acquisition and procurement programs and enterprise services, must have a net ready key performance parameter (NR KPP) as part of its interoperability requirements documentation.

- IT must be certified for interoperability, or possess an interim certificate to operate (ICTO) or waiver to policy before connection to any DoD network (other than for test purposes).
DoD Instruction 8330.01
Interoperability of IT, Including National Security Systems

• Updated/replaced DoD’s 10 year old interoperability policies (DoDD/DoDI 4630)
• Established policy, assigned responsibilities, and provided direction for certifying the interoperability of IT
  – Requires Interoperability Certification prior to connection to a DoD network
  – Establishes 2 tiers of interoperability certification:
    • For IT with joint, multinational, or interagency interoperability requirements: Joint Staff certifies the NR KPP, JITC tests and certifies the system against the NR KPP
    • For all other IT: individual DoD Components certify the NR KPP, and test and certify the system against the NR KPP
  – Streamlined the ISP review process
  – Formally established the Interoperability Steering Group (ISG) to provide oversight
• Signed by Acting DoD CIO 21 May 2014
DoD CIO

Interoperability Governance

The Interoperability Steering Group (ISG):

- Replaces both the Military Communications Electronics Board’s ICP and IP
- Is subordinate to the CIO Executive Board
- Is tri-chaired by representatives from DoD CIO, AT&L, and CJCS
- Proposes, reviews, and coordinates interoperability policies; reviews critical interoperability issues; and adjudicates requests for Interim Certificates to Operate (ICTOs) and waivers to policy
DoD Interoperability Steering Group (ISG)

- **Purpose**: Provides a forum to coordinate policy and provide oversight and direction across DoD organizations in ensuring the interoperability of IT and NSS. The ISG proposes, reviews, and coordinates interoperability policies; reviews interoperability issues; and reviews and approves requests for Interim Certificates to Operate (ICTOs) and waivers to policy.

- **Tri-chaired by representatives from the DoD CIO, USD (AT&L), and the CJCS**

- **Meets every other month in person—handles routine ICTO and waiver requests out-of-cycle**

- **Value added**: 

<table>
<thead>
<tr>
<th>CY</th>
<th>ICTOs</th>
<th>Waivers</th>
<th>Joint IOP Certs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>310</td>
<td>116</td>
<td>252</td>
</tr>
<tr>
<td>2012</td>
<td>232</td>
<td>114</td>
<td>314</td>
</tr>
<tr>
<td>2013</td>
<td>158</td>
<td>32</td>
<td>319</td>
</tr>
<tr>
<td>2014 (to date)</td>
<td>119</td>
<td>32</td>
<td>234</td>
</tr>
</tbody>
</table>
DoD CIO

IT Interoperability Certification and Connection Process

**IT Joint, Multinational, and Interagency Interoperability Certification and Connection Process**

Performed Prior to Fielding Decision and Connection to the Network (and repeated before each ATC/IATC renewal)

- **Program Manager (through Component):** Provides ISP (with Certified NR KPP) and Component results of non-joint interface testing.

- **JITC:** Coordinates Interoperability Test and Evaluation Strategy

- **Milestone Decision/Fielding Decision Authority:**
  - Evaluates any External Interoperability Test Data (as required)
  - Conducts Interoperability Testing (as required)
  - Grants Joint Interoperability Certification

- **Connection Approval Office:**
  - Integrates Interoperability Certification into Milestone Decision and/or Connection Request Package
  - Updates Authoritative IT Registry
  - Proceeds with Milestone/Fielding Decision
  - Proceeds with Connection Decision
DoD Interoperability Process Guide (IPG)

- Outlines the procedures and documentation required for Joint Interoperability Test and Certification, waiver processing, and associated processes and procedures

- *IPG Version 1* was jointly signed by DISA T&E Executive and Director A&I in 2012

- *Change 1* to the IPG issued to update and revise the IPG to include:
  - Fact-of-life changes
  - Updated waiver and Interim Certification to Operate processes
  - Operating at Risk List processes
  - Guidance to define the minimum architecture data needed for interoperability certification

- Status:
  - *IPG Version 1 Change 1* was co-signed by DISA Test & Evaluation Executive and Acting DCIO(IE) PD 30 April 2014
## Architecture Viewpoints Required for Interoperability Certification

<table>
<thead>
<tr>
<th>Viewpoint</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>REQUIRED Architecture Viewpoints for Joint Interoperability Certification</strong></td>
<td></td>
</tr>
<tr>
<td>AV-1</td>
<td>Overview of architecture scope and context, describes the concepts contained in the OV-1.</td>
</tr>
<tr>
<td>AV-2</td>
<td>Integrated Dictionary – defines all terms and metadata used in the architecture.</td>
</tr>
<tr>
<td>OV-1</td>
<td>High Level Operational Concept Graphic – describes operational concept.</td>
</tr>
<tr>
<td>OV-2</td>
<td>Operational nodes, needlines, and activities - information exchanges between operational nodes.</td>
</tr>
<tr>
<td>OV-3</td>
<td>Information exchanges and associated measures and metrics.</td>
</tr>
<tr>
<td>OV-5b</td>
<td>Operational Activity Model - NR KPP Missions/Tasks - activity level depiction.</td>
</tr>
<tr>
<td>OV-6c</td>
<td>Event-Trace Description - lifelines (nodes) and events.</td>
</tr>
<tr>
<td>SV-1</td>
<td>Systems Interface Description - defines system functions and information flow among systems.</td>
</tr>
<tr>
<td>SV-2</td>
<td>Systems Resource Flow Description - communications links, networks, and systems.</td>
</tr>
<tr>
<td>SV-5a</td>
<td>Maps system functions (activities) to operational activities.</td>
</tr>
<tr>
<td>SV-6</td>
<td>System data exchanges &amp; associated measures and metrics.</td>
</tr>
<tr>
<td>SV-7</td>
<td>Complete set of system performance parameters (measures).</td>
</tr>
</tbody>
</table>

| **CONDITIONAL Architecture Viewpoints for Joint Interoperability Certification** | |
| DIV-2 | Logical Data Model - architecture data definitions. |
| DIV-3 | Physical Data Model - describes how DIV-2 is implemented. |
| StdV-1 | Standards Profile - list of implemented technical standards, rules, and guidelines. |
| SV-5b | Maps systems to operational activities. |
| SvC-1 | Services Context Description – identifies services and their interconnections. |
| SvC-2 | Specifies resource flows exchanged between services, and may list protocol stacks. |
| SvC-4 | Depicts allocation of service functions and data flows between service functions (activities). |
| SvC-5 | Maps services (activities) to operational activities. |
| SvC-6 | Maps service data exchanges with associated measures and metrics. |
| SvC-7 | Complete set of performance parameters (measures) of the services. |

| **OPTIONAL Architecture Viewpoints for Joint Interoperability Certification** | |
| CV-all | Capability Viewpoints – taxonomy, capability evolution, etc. |
| OV-4 | Key architecture players and organizational relationships. |
| OV-5a | Describes capabilities and operational activities. |
| PV-all | Project capability delivery and dependencies. |
| StdV-2 | Emerging standards (may be conditional if emerging standards are implemented and not in StdV-1). |
| SV-4 | Defines data flow input and output by each function (activity). |