Joint Capabilities Integration and Development System (JCIDS) 
A Primer

Sources:
• CJCSI 5123.01H, 31 Aug 2018
• JCIDS Manual, 31 Aug 2018
• DoDI 5000.02, 7 Jan 2015, change 4

Patrick Wills
Dean, Defense Systems Management College
Defense Acquisition University
work: 703-805-4563 cell: 703-615-5234
31 Jan 2019
• The Requirements Environment
• JCIDS & DoD Decision Support Systems
• JROC Capability Requirements Documents
• JCIDS Process Lanes & the Deliberate Lane
• Identifying & Documenting Capability Requirements and Gaps (Capabilities-Based Assessment to Production)
• Performance Attributes
• Information Systems (IS) and the “IT Box”
• Intelligence Supportability
• DOTmLPF-P Content
• Weapons Safety Assurance
• Document Staffing and Validation
• Urgent Need Lanes
• Guiding Principles and Challenges

Select topic on left and return to topic list as desired.

If you are new to JCIDS review some useful terms here
Finding the balance between:

Combatant Command (CCMD) near-term requirements to support Contingency Plans and current missions and Services’ long range vision & investment plans

Versatile, joint systems and Systems optimized for service missions

Growing demands and Fiscal & political constraints

Geographic specificity and Worldwide applicability

Ambitious requirements and Achievable acquisition strategy

Quantity matters and High-end capabilities
The Requirements & Acquisition Challenge

Implement The National Defense Strategy

• Build a More Lethal Force
  – Modernize capabilities
  – Innovative operational concepts
  – Cultivate workforce talent

• Strengthen Alliances and Attract New Partners

• Deepen interoperability

• Reform the Department for Greater Performance and Affordability
  – Deliver Performance at the speed of relevance
    ➢ Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting
  – Drive budget discipline and affordability to achieve solvency
  – Streamline rapid, iterative approaches from development to fielding
  – Harness and protect the National Security Innovation Base
JCIDS Role in DoD Decision Support Systems
Joint Capabilities Integration and Development System (JCIDS)

JCIDS Provides...

• The primary means for the Joint Requirements Oversight Council (JROC) to fulfill its statutory responsibilities to the Chairman of the Joint Chiefs of Staff (CJCS). These responsibilities include assessing joint military capabilities, and identifying, approving, and prioritizing gaps in these capabilities, to meet applicable requirements in the National Defense Strategy (NDS).

• The baseline for documentation, review, and validation of capability requirements across the Department.

JCIDS along with the Defense Acquisition System and the Planning, Programming, Budgeting and Execution process form the principal DOD decision support processes for developing and acquiring capabilities required by the military forces to support the National Defense Strategy.

See notes page for more information
DoD’s Three Decision Support Systems

**Big “A” Acquisition**
- USD (A&S) / USD (R&E) Oversight
- Traceable Requirements Decomposition
- Thorough Systems Engineering & Testing
- Delivers Capability to Warfighter

**Event Driven (DoD 5000.01/02)**
- USD(A&S) / USD(R&E) Oversight
- Traceable Requirements Decomposition
- Thorough Systems Engineering & Testing
- Delivers Capability to Warfighter

**Need Driven (CJCSI 5123.01/JCIDS Manual)**
- CJCS Oversight
- Capability & Gap Analysis
- Major Documents (ICD, CDD, DCR)
- Joint Focus; Capability-based approach

**Calendar Driven (DoDD 7054.14)**
- USD(C) / Dir CAPE Oversight
- Budgeting to Support Development, Procurement, & Sustainment

**Proper synchronization delivers timely and relevant capabilities to the Warfighter**

- DCR: DOTMPLF-P Change Recommendation
- ICD: Initial Capabilities Document
- CDD: Capability Development Document
- USD(C): Under Secretary of Defense (Comptroller)
- Dir CAPE: Cost Assessment and Program Evaluation
- DAS: Defense Acquisition System
- JCIDS: Joint Capabilities Integration & Development System
- PPBE: Planning, Programming, Budgeting & Execution
- USD(A&S): Under Secretary of Defense (Acquisition & Sustainment)
- USD(R&E): Under Secretary of Defense (Research & Engineering)
JCIDS – The Central Process
For Joint Capability Solutions

Current Joint Warfighting Capabilities

- Assess current capabilities
- Identify gaps
- Identify capability requirements
- Recommend non-materiel and/or materiel approaches

Future Joint Warfighting Capabilities

- Strategic Guidance
- Joint Concepts
- CONOPS

Warfighter Feedback

Non-Materiel Solutions

Accept Risk
Do nothing

JCIDS

Recommended Materiel Approaches

Resources

- PPBE
- Congress

Acquisition

- Determine Materiel Solution
- Estimate Cost & obtain funding
- Design, Develop & Test
- Produce & Field

See notes page for more information
Joint Requirements Oversight Council (JROC)

Chair: Vice Chairman JCS

Council Members:

- Vice Chief of Staff, Army
- Vice Chief of Naval Operations
- Vice Chief of Staff, Air Force
- Assistant Commandant of the Marine Corps

Advisors to the JROC:

- Under Secretaries of Defense (USD): USD(Acquisition & Sustainment), USD(Research & Engineering), USD(Policy), USD(Intelligence), and USD(Comptroller)
- Director, Cost Assessment & Program Evaluation (CAPE)
- Director, Operational Text & Evaluation (DOT&E)
- Commander of a Combatant Command when matters related to the area of responsibility or functions of that command are under consideration.
JCIDS Capability Requirements Documents
Materiel Solutions

• **Initial Capabilities Document (ICD)**
  – The identification of capability requirements with significant capability gaps typically leads to an ICD that can then drive development of capability solutions that are materiel, non-materiel, or a combination of both.
  – Specifies capability requirements in terms of mission-level operational attributes
  – The most common starting point to document capability requirements when a materiel approach is deemed appropriate.
  – Typically leads to an AoA and then the CDD for development of a materiel solution.

• **Capability Development Document (CDD)**
  – Capability requirements document tailored toward a materiel approach for a capability solution and also includes nonmateriel aspects of the materiel solution.
  – Specifies capability requirements, in terms of system level performance attributes which include Key Performance Parameters (KPPs), Key System Attributes (KSAs), and Additional Performance Attributes (APAs) to support development of one or more increments of a materiel capability solution.
• Joint DOTmLPF-P Change Requests (Joint DCRs)
  – Identifies non-materiel approaches to closing capability gaps and meeting joint military
capability requirements, including capability requirements being satisfied by Services
contracting (DoDI 5000.74).
  – May be generated from one or more validated ICDs as a non-materiel solution to validated
capability requirements and associated capability gaps, or as a complement to a materiel
capability solution, which will be developed through the acquisition process.
  – May be generated without an associated ICD if non-materiel approaches appear to be the most
viable solution for identified capability requirements.
  – The letter “m” in the acronym is lower case, since Joint DCRs do not advocate new materiel
development, but rather advocate increased quantities or alternate applications of existing
materiel to include Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS), or
Non-Development Items (NDI).

DoD Components manage Component-specific non-materiel changes at their discretion.
JCIDS Capability Requirements Documents
Urgent/Emergent Need Documents

• Joint Urgent Operational Need (JUON).
  – Capabilities that are driven by ongoing contingency operations that are necessary to prevent loss of life or critical mission failure that require out-of-cycle funding to initiate program execution.

• Joint Emergent Operational Need (JEON)
  – Capabilities that are driven by anticipated contingency operations necessary to prevent loss of life or prevent critical mission failure, and where out-of-cycle funding is required to initiate program execution.

DoD Component UONs are applicable to only one DoD Component guided by ongoing or anticipated contingency operations. Component UONs are submitted, staffed, and validated IAW Component policy.
JCIDS Process Lanes & the Deliberate Lane
### JCIDS Process Lanes

<table>
<thead>
<tr>
<th>JCIDS Lanes</th>
<th>Operational Timeline</th>
<th>JCIDS Documents</th>
<th>JCIDS Staffing Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ongoing Contingency Lane</strong></td>
<td>Urgent Need (&lt;2 Years)</td>
<td>JUON</td>
<td>15 days</td>
</tr>
<tr>
<td><strong>Anticipated Contingency Lane</strong></td>
<td>Emergent Need (&lt;2Years)</td>
<td>JEON</td>
<td>31 days</td>
</tr>
<tr>
<td><strong>Deliberate Lane</strong></td>
<td>Future Need (&gt;2Years)</td>
<td>ICD  CDD</td>
<td>97 days 103 days</td>
</tr>
</tbody>
</table>

- **Ongoing Contingency Lane - Urgent Need**
  - Urgent need to prevent loss of life and/or mission failure during current operations
- **Anticipated Contingency Lane - Emergent Need**
  - Accelerated acquisition needed for an anticipated or pending contingency operation
- **Deliberate Lane – Future Need**
  - Traditional route for capabilities that require significant tech development and/or are not urgent or compelling in nature
**JCIDS Process Lanes**

<table>
<thead>
<tr>
<th>JCIDS Lanes</th>
<th>Operational Timeline</th>
<th>JCIDS Documents</th>
<th>JCIDS Staffing Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ongoing Contingency Lane</strong></td>
<td>Urgent Need (&lt;2 Years)</td>
<td>JUON</td>
<td>15 days</td>
</tr>
<tr>
<td><strong>Anticipated Contingency Lane</strong></td>
<td>Emergent Need (&lt;2 Years)</td>
<td>JEON</td>
<td>31 days</td>
</tr>
<tr>
<td><strong>Deliberate Lane</strong></td>
<td>Future Need (&gt;2 Years)</td>
<td>ICD CDD</td>
<td>97 days 103 days</td>
</tr>
</tbody>
</table>

- **Deliberate Lane – Future Need**
  - Service, CCMD or Agency Driven. Traditional route for capabilities that require significant tech development. Uses the ICD to validate joint military capability requirements and the CDD to validate proposed capability solutions.
- **The next series of charts deal with the Deliberate lane**
JCIDS and the Defense Acquisition System

Hardware Intensive Program Model, DoDI 5000.02

- **Materiel Development Decision (MDD)**. Validated ICD supports MDD, MSA Phase and informs conduct of an AoA.
- **Milestone A and TMRR Phase**. Draft CDD (approved by Sponsor; not submitted to Joint Staff).
- **Development Request for Proposal (RFP) decision, Milestone B, and EMD Phase**. Validated CDD.
- **Milestone C, LRIP, FRP/FD Decision, and the P&D Phase**. Validated (updated if necessary) CDD.

For a more detailed illustration go [here](#) (slide show mode)
• Identification of Capability Requirements & Gaps
• Capabilities-Based Assessment (CBA)
• JCIDS Support, MDD to Full Rate Production
Identification of Capability Requirements and Associated Capability Gaps

• **Purpose.** To derive and refine joint military capability requirements and associated capability gaps – for which a capability solution must be provided either organically or leveraged through the joint force – to accomplish assigned functions, roles, missions, and operations.

• **Certified Requirements Managers.** Sponsors will use certified requirements managers to monitor and evaluate capability requirement identification, including but not limited to the identification of capability gaps due to changes in threats, missions, or aging of legacy weapon systems throughout their life cycle.

• **Relation to Functions, Roles, Missions, and Operations.** Before any action can be taken in the JCIDS process related to reviewing and validating capability requirement documents, Sponsors must first identify capability requirements related to their functions, roles, missions, and operations.

See notes page for more information
Approaches to Identifying Capability Requirements

• Capabilities-Based Assessments (CBAs)
• DOTmLPF-P Analysis
• Other Studies and Analysis
  – Operational Planning
  – Exercises/Warfighting Lessons Learned
  – Joint Capability Technology Demonstrations (JCTDs) and Other Experiments
  – Transition of Rapidly Fielded Capability Solutions
  – Joint Urgent Operational Needs (JUONs), Joint Emergent Operational Needs (JEONs), and DOD Component Urgent Operational Needs (UONs)
  – Business Process Reengineering

See notes page for more information
Considerations of Approaches to Identify Capability Requirements

- Mission Description & Military Problem Being Assessed
- Identification & Assessment of Prior Studies
- Identification of Tasks Required to Meet Mission Objectives
- Identification of Joint Military Capability Requirements Within One or More Joint Capability Areas (JCAs)
- Assessment of Capability Gaps
  - Between identified requirements and current or programmed joint force capabilities
- Assessment of Operational Risks
- Evaluation of Possible Non-Materiel & Materiel Approaches to Close or Mitigate Gaps
- Evaluation of Current and Potential Future Science & Technology (S&T) Efforts
- Recommendation for the Most Appropriate Approach to Close or Mitigate Capability Gaps and Reduce Operational Risk
The “Capability Mission Lattice” (CML) provides an integrating construct for articulating the dependencies between capability requirements as well as the traceability between related processes and activities across the department.

For the full-size version go [here](#) (use slide show).
Capabilities-Based Assessment (CBA)

Existing Guidance

Needs Analysis

What we need
For the mission

Gap Analysis

Problems and Risks

Solutions Analysis

What should we do about it?

Where does this need rank?
How soon do we need it?

See notes page for more information
From Strategic Guidance to Future Capabilities

- **Strategic Guidance**
- **Capstone Concept for Joint Operations**
  - CONOPS & Threat
  - SSA Products
- **Joint Operating Concepts**
- **Supporting Joint Concepts**
- **Capabilities-Based Assessment or other study**
  - Identifies capability requirements and gaps
- **Future Joint Warfighting Capabilities**
  - Recommends non-materiel and/or materiel approaches
- **ICD/DCR**

**Family of Joint Concepts**
Getting The Front End Right is Key

MDD

CBA or Other Study

ICD

Front End, Defense Acquisition System

See notes page for more information
CBA Outputs

• CBA Results Documentation:
  – Initial Capabilities Document (ICD)
  – Joint DOTmLPF-P* Change Recommendation (DCR)

• CBA Recommendations for Materiel Approaches:
  – Evolution of fielded solutions with significant capability improvement, to include information systems
  – Replacement or recapitalization of previously fielded system with significant capability improvement
  – Introduction of a transformational capability solution(s) that differ significantly in form, function, operation, and capabilities from previously fielded systems
  – Increase integration/interoperability of existing capabilities to create new System of Systems.

• Managers Must Communicate to Avoid Disconnects Over Seams Between JCIDS, Defense Acquisition System, and Planning, Programming, Budgeting, and Execution (PPBE)

See notes page for more information
CBA Output Document – ICD

• Initial Capabilities Document (ICD) (Includes the Information Systems (IS) Variant)
  – Documents Capabilities-Based Assessment (CBA) results
  – Specifies one or more capability requirements and associated capability gaps which represent unacceptable operational risk if left unmitigated
  – Identifies relevant operational attributes
  – Identifies notional resources available over anticipated life cycle
  – Recommends partially or wholly mitigating identified capability gap(s) with a non-materiel capability solution, materiel capability solution, or some combination of the two
  – Supports the Materiel Development Decision (MDD)
  – Predecessor for the Capabilities Development Document (CDD)

• Page Limit, Document Body: 10 Pages
ICD Operational Attributes

• An ICD Identifies Capability Requirements – Operational Attributes with Associated Initial Objective Values
  – Operational Attributes are mission related Measures of Effectiveness
  – Initial objective values are the values necessary to achieve mission objectives with moderate operational risk.
  – Examples: Outcomes, time, distance, effect, obstacles to be overcome, and supportability

• Guides the Analysis of Alternatives (AoA) conducted during the Materiel Solution Analysis Phase

• With AoA results, Guides Development of Performance Attributes (KPP, KSA and APA) for the Capability Development Document (CDD)
CBA Output Document – Joint DCR

• Joint DOTmLPF-P Change Recommendation (Joint DCR)
  – To propose joint non-materiel solutions as an alternative to, or complement of, materiel solutions
  – Non-Materiel Solutions
    ➢ Alternate concepts and CONOPs
    ➢ Organizational and personnel alternatives to resolve gaps/mismatches between force availability and force needs
    ➢ Training changes that improve effectiveness of existing capabilities
    ➢ Alternate uses of previously fielded materiel
    ➢ Leadership and educational alternatives
    ➢ Use existing facilities in new ways; introduce new facilities or locations
    ➢ Policy alternatives – change policies that contribute to gaps in capability

• Page Limit, Document Body: 30 Pages

For non-materiel solutions which impact only the Sponsor organization, DCRs are not required
DOD Components manage Component specific DOTmLPF-P changes at their discretion.
JCIDS and the Defense Acquisition System
This chart illustrates the flow of operational context and capability requirement and gap data gathered during a CBA to the ICD/CDD.

See the JCIDS Manual for the full range of required DODAF data for JCIDS documents.
Post-Analysis of Alternatives (AoA) Review

• The post-AoA review provides the validation authority and other stakeholders the opportunity to assess how different alternatives address validated capability requirements and associated capability gaps, and at what life cycle costs.

• Must be completed in time to permit Sponsor preparation of a draft CDD prior to Milestone A, not submitted to the Gatekeeper for staffing and validation at that time, to inform development of request for proposal (RFP) in support of TMRRR Phase.

• The post-AoA review is not a validation of AoA results, but rather informs the validation authority’s advice to the MDA on AoA results, recommended alternative(s), and proposed KPPs, KSAs, and APAs.
  – The validation authority may recommend alternative(s) different from those recommended by the sponsor when such a recommendation would better serve the management and prioritization of the capability requirements portfolio.

• Upon completion of the Post-AoA review, the validation authority for all MDAPs will provide a JROCM or component level memorandum that endorses the AoA results and provides recommendations to the MDA.
Key JCIDS Document - CDD

• Capability Development Document (CDD)
  – Proposes development of a specific materiel solution
  – *Draft CDD (Sponsor Approved)* supports Milestone A and Technology Maturation and Risk Reduction (TMRR) Phase
  – Validated CDD supports Development RFP Release Decision, Milestone B, EMD Phase, Milestone C, and Production and Deployment Phase
  – Identifies performance attributes:
    - KPPs, Key System Attributes (KSAs), and Additional Performance Attributes (APAs)
    - Other System Attributes, such as Human Systems Integration (HSI), environmental factors, transportability, etc..
  – Describes DOTmLPF-P considerations associated with the solution
  – May apply to multiple increments of development

• Page Limit, Document Body: 45 Pages

CDD KPPs are inserted verbatim into the Acquisition Program Baseline (APB)
CDD & Incremental Paths

• **Incremental Development.**
  – Sponsor describes the system and performance attributes of the initial capability solution in a base CDD. As incremental capability is added to the base system over time, or block upgrades are developed, the Sponsor may document this in an annex to the base CDD.

• **Family of Systems (FoS)**
  – In an FoS approach with a single Sponsor, the Sponsor may develop a base CDD and concurrently staff annexes for individual systems within the family. The base CDD will specify attributes for the entire FoS and each annex will specify additional attributes for the individual systems.

Family of Systems (FoS) - A set of systems that provide similar capabilities through different approaches to achieve similar or complementary effects. For example, the warfighter may need the capability to track moving targets. The FoS that provides this capability could include manned or unmanned aerial vehicles (UAVs) with the appropriate sensors, a space based platform or special operations capability.
Configuration Steering Boards (CSB)

“... the Acquisition Executive of each DoD Component will form and chair a CSB with broad executive membership . . .”

DoDI 5000.02, Jan 2015, change 4

- CSBs meet at least annually
  - Review all requirements changes and significant technical configuration changes with potential for cost and schedule impacts
  - Only approve changes that increase cost if funds identified and schedule impacts addressed.
  - Requirements fall under CSB cognizance once CDD is validated
- The CSB monitors changes in program requirements and ensures that Service Chief, in consultation with the Secretary of the Military Department and the JROC, approves of any proposed changes that could have an adverse effect on program cost, schedule, or performance.
- The PM (with the PEO) identifies descoping options to reduce program cost or to moderate requirements
- CSB recommends to the MDA and requirements validation authority which options should be implemented
JCIDS and the Defense Acquisition System
Key JCIDS Document Production

• Capability Development Document (Updated CDD)
  – Proposes production of an increment of a specific materiel solution
  – Supports Milestone C
  – Identifies production performance attributes:
    ➢ KPPs, KSAs, and APAs
    ➢ Other System Attributes, such as Human Systems Integration (HSI), environmental factors, transportability, etc.
  – Identifies DOTmLPF-P impacts of the solution
  – Does not introduce new requirements

• Page Limit, Document Body: 40 Pages

CDD KPPs are inserted verbatim into the APB for Milestone C
Performance Attributes
Performance Attributes

• Performance attributes are characteristics or inherent parts of a system required for the system to achieve satisfactory performance.
  – Key Performance Parameters (KPPs)
  – Key System Attributes (KSAs)
  – Additional Performance Attributes (APAs)

• Sponsors must establish KPPs, KSAs, and APAs which are technically achievable, quantifiable, measurable, testable, unambiguous, supported by documented trade-off analysis, and defined in a manner that supports efficient and effective T&E.

• The number of performance attributes should be kept to a minimum to maintain program flexibility.

• Performance attributes listed in the capability requirements documents that have joint equity will be designated by the Joint Staff Gatekeeper as Joint Performance Requirements (JPRs).
Key Performance Parameters (KPPs)

• Performance Attributes of a system critical or essential to development of an effective military capability

• Validated by JROC for JROC Interest Documents
  – Change authority generally retained by the validation authority, unless specifically delegated in the validation memorandum.

• Failure to meet a validated KPP threshold triggers a review by the validation authority and evaluation of operational risk and/or military utility of the system(s).
  – Review may result in validation of an updated KPP threshold value, modification of production increments, or recommendation for program cancellation.
Key System Attributes (KSAs)

- Performance attributes considered important to achieving a balanced solution
- Not critical enough to be selected as a KPP
- Identified by the sponsor; should be kept to a minimum
- Change authority delegated to Sponsor, unless retained in document validation memorandum
Joint Performance Requirements (JPRs)

- **Joint Performance Requirements (JPRs)** are performance requirements critical or essential to ensure interoperability or fulfill a capability gap of more than one armed force, Defense Agency, or other entity of the Department of Defense, or impacts the joint force in other ways such as logistics.
- Upon initial staffing, Sponsor will recommend whether a KPP should be designated a JPR.
- If not already determined to be a KPP, all performance attributes designated JPRs will be upgraded to a KPP.
- Final JPR designation will be made by the validation authority when the capability requirements document is validated.
Mandatory Performance Attributes

- **Mandatory Performance Attributes**
  - Four mandatory KPPs as well as the Net-Ready Performance Attribute.

- **Mandatory KPPs** - attributes that are designated as mandatory KPPs IAW Title 10 US Code:
  - Force Protection
  - System Survivability
  - Sustainment
  - Energy

- Neither the mandatory KPPs nor the net-ready performance attribute are applicable to every capability requirement. If the Sponsor determines that a mandatory KPP or the net-ready performance attribute is not applicable to their operational context, the Sponsor must articulate the reason(s) why.
Mandatory Performance Attributes
KPPs & Supporting KSAs

• **Force Protection KPP** *(CDDs for manned systems or systems designed to enhance personnel survivability).* Intended to ensure protection of occupants, users, or other personnel who may be adversely affected by the system or threats to the system.

• **System Survivability KPP** *(all CDDs).* Intended to promote the development of critical warfighter capabilities that can survive kinetic (i.e., traditional, non-traditional, and CBRN (including EMP)) and non-kinetic (cyber and EMS)) threats across domains and applicable environments including space.

• **Sustainment KPP** *(all CDDs).* Intended to ensure an adequate quantity of the capability solution will be ready for tasking to support operational missions. Mandatory Components:
  - Materiel Availability (KPP)
  - Operational Availability (KPP)
  - Reliability (KSA or APA) (may include more than one metric, e.g. mission reliability and logistics reliability). N/A to Automated Information Systems (AIS)
  - Operation & Support Costs (KSA or APA)

• **Energy KPP** *(CDDs that specify capabilities that use operational energy or consume energy to sustain performance over scenario timelines).* Intended to ensure combat capability of the force by balancing the energy performance of systems and the provisioning of energy to sustain systems/forces required by the operational commander under applicable threat environments.
Mandatory Performance Attribute
Force Protection (FP) KPP

• **Application.** CDDs for –
  - Manned systems, unmanned systems which interface with or operate in the proximity of personnel, and for systems designed to enhance personnel survivability

• Force Protection attributes include protection from –
  - Kinetic fires
  - Non-kinetic fires
  - CBRN effects
  - Environmental effects
  - Crash events

• Synergy/overlap with System Survivability (SS) KPP –
  - May include same attributes as the SS KPP, but emphasis is on protecting occupants / other personnel rather than protecting the system itself.

• Exclusion of offensive attributes: Offensive attributes primarily intended to defeat adversary forces before they can engage non-adversary forces are not included as part of the FP KPP.

• **Proponent.** Protection FCB

See notes page for more information
Mandatory Performance Attribute
System Survivability (SS) KPP

• **Application.** All CDDs, including IS-CDDs

• Promotes development of critical warfighter capability that can survive kinetic (i.e., traditional, non-traditional, and CBRN) and non-kinetic (cyber and electromagnetic spectrum (EMS)) threats across domains and applicable environment including space

• Supports three system oriented objectives: prevention, mitigation in tactically relevant time, and recovery from threats and fires. Simultaneously, the SS KPP maintains survivability from diverse environmental factors (i.e., heat, dust, moisture, EMS-congested areas, etc.).

• **Scope.** Three focus elements: Kinetic Survivability, Cyber Survivability, and EMS Survivability. Not all systems will need to comply with the requirements of all three-focus areas.

• **Proponent.** Protection FCB

See notes page for more information
Mandatory Performance Attribute
Sustainment KPP & KSAs

• **Application.** All CDDs.

• The value of the Sustainment KPP is derived from the capability requirements of the system, assumptions for its operational context and intended use, and planned logistical support. Fully developed sustainment objectives allow the PM to develop a solution to satisfy the warfighter requirements and system performance to be measured against standardized metrics.

• **Mandatory Components:**
  – Materiel Availability and Operational Availability (KPPs)
  – Reliability (Mission and Logistics) (KSAs or APAs)
  – Maintainability (KSA or APA)
  – Operations & Support Cost (KSA or APA)

• **Optional.** Logistics Footprint

• **Proponent.** Joint Staff, J-4/ Maintenance, Materiel, and Services Division)

See notes page for more information
Mandatory Performance Attribute
Energy KPP

• **Application.** CDDs that specify capabilities that use operational energy or consume energy to sustain performance over scenario timelines. Differs from other KPPs in several ways:
  
  – Fuel delivery logistics (tanker aircraft, oilers, and fuel trucks) have a uniquely large presence in the total force structure and in the battlespace.
  
  – Fuel, in the large volumes U.S. forces demand it, and, in the timeframe when new systems will come into the force, may become less readily available for procurement in proximity to where it is required for operations.
  
  – The Energy KPP does not focus directly on energy-related costs, but rather on mission effectiveness within the context of mission and threat.

• The Energy KPP is intended to ensure combat capability of the force by balancing the energy performance of systems and the provisioning of energy to sustain required systems/forces by the operational commander in relevant threat environments.

• **Proponent.** Joint Staff J-4 / Engineering Division (J-4/ED)
Mandatory Performance Attribute
Net Ready

- **Application.**
  - Capability Requirements and Gaps/Overlaps section of the IS-ICD
  - Joint Interoperability Section of the CDD and IS-CDD
  - JUON, JEON, and DoD Component UON IT solutions fielded and proposed for transition to enduring use.
  - Not Applicable to Systems That Do Not Communicate With External Systems

- **Net-Ready Content:**
  - Criteria for interoperability, and operationally effective end-to-end information exchanges traceable to their associated operational context, and are technically achievable, quantifiable, measurable, testable, unambiguous, supported by documented trade-off analysis, and defined in a manner that supports efficient and effective T&E.

- **Proponent.** C4/Cyber FCB

See notes page for more information
Net-ready content includes three attributes derived through a three-step process* of mission analysis, information analysis, and systems engineering and architecture.

- **Attribute 1. Support to military operations.** Specifies which military operations (e.g., missions or mission threads), as well as operational tasks, a system supports. Threshold and objective values of MOEs are used to measure mission success. Threshold and objective values of MOPs are used to measure task performance.

- **Attribute 2. Entered and be managed on the network.** Specifies which networks the system must connect to in order to support military operations.

- **Attribute 3. Exchange information.** Specifies the information elements produced and consumed by each mission and net-ready operational task identified above.

*Figure B-17, JCIDS Manual Depicts this Three-Step Process

See notes page for more information
For an IS-ICD, Section 3 includes a Net Ready Attribute Table depicting performance parameters for three attributes: Support to Military Operations, Enter and Manage in the Network, and Exchange Information.

### Attribute: Support to Military Operations

<table>
<thead>
<tr>
<th>NR Performance Attribute</th>
<th>Performance Parameter¹</th>
<th>Initial Minimum Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support to Military Operations</td>
<td>Mission: Security Qualitative Capability (SQC)² Mission is to plan, request, coordinate, and control Close Air Support (CAS) missions, and provide C2 situational awareness, in support of joint and coalition ground maneuver forces. Mission Activity: Provide voice and data communications with mission partners. Measure: Accuracy of SQC information; consistently processed, stored, and made available to user or external consumer exactly as obtained. Mission Activity: Provide situational awareness. Measure: Accuracy of mission update messages from other C2 platforms. Conditions: Adverse weather, day/night air transport operations in permissive to low threat environment</td>
<td>&gt; 99%</td>
</tr>
</tbody>
</table>

¹ **Bold Text is the template; non-bold and italicized text provides an example.**
² Security Qualitative Capability (SQC) is a fictitious program for purposes of this example
### Attribute: Enter and Manage in the Network

<table>
<thead>
<tr>
<th>NR Performance Attribute</th>
<th>Performance Parameter</th>
<th>Initial Minimum Value</th>
</tr>
</thead>
</table>
| Enter and Manage in the Network | **Network:** NIPRNET. **Measure:** Time to connect to an operational network from power up. **Network:** SIPRNET. **Measure:** Time to connect to an operational network from power up. **Network:** Link-16. **Measure:** Time to connect to an operational network from power up. **Measure:** Availability of network during adverse weather conditions. **Condition:** Continuous Network Connectivity based on system-controllable factors. | ≥ 1 minute  
≥ 5 minutes  
≥ 2 minutes  
≥ 99% |

1 **Bold Text is the template; non-bold and italicized text provides an example.**
### Attribute: Exchange Information, example

<table>
<thead>
<tr>
<th>NR Performance Attribute</th>
<th>Performance Parameter</th>
<th>Initial Minimum Value</th>
</tr>
</thead>
</table>
| **Exchange information** | **Information Element:** Support Data.  
Measure: Time to exchange data between SQC and System A (NGA).  
**Information Element:** Target Data.  
Measure: Time to exchange data between SQC and System B (NSA).  
**Information Element:** ISR Data.  
Measure: Time to exchange data between SQC and System C (USCENTCOM).  
**Conditions:** NSA Type 1 Certified Encryption  
Systems in operation and continuous network connectivity | ≥ 2 minutes  
≥ 2 minutes  
≥ 2 minutes |

---

1 **Bold Text is the template; non-bold and italicized text provides an example.**  
2 Security Qualitative Capability (SQC) is a fictitious program for purposes of this example.
Additional Performance Attributes (APAs)

- Performance Attributes of a System Not Important Enough to be a KPP or KSA
- Must be measurable, testable, and support efficient and effective T&E
- Identified by the Sponsor; should be kept to a minimum
- Change authority delegated to Sponsor, unless retained in document validation memorandum
Thresholds, Objectives, and Trade Space

• Performance attributes are expressed in threshold / objective format.
  – **Thresholds.** Threshold values must be achievable within the projected lifecycle cost, schedule, and technology at low-to-moderate risk. Performance below the threshold value is not operationally effective or suitable or may not provide any improvement over current capabilities.
  – **Objectives.** The objective values are applicable when a higher level of performance represents significant increase in operational utility. Context must be provided to articulate what operational impact or risk is further mitigated if the performance were to reach the objective value. If applicable, the objective value is the desired operational goal achievable, but at higher risk in lifecycle cost, schedule, and technology. Performance above the objective value does not justify additional expense.

• **Trade Space.** The difference between threshold and objective values sets trade space for balancing multiple KPPs, KSAs, and APAs while remaining above the threshold values.
Other System Attributes

- Other system attributes not directly quantified as performance attributes, and not identified elsewhere in the CDD.
- May include, but not limited to:
  - Future integration platforms
  - Embedded instrumentation, electronic attack, and wartime reserve mode requirements.
  - Human Systems Integration (HSI) considerations.
  - Natural environmental factors, including climatic design type, terrain, meteorological and oceanographic factors.
  - Physical and operational security needs, including technology security, foreign disclosure, defense exportability feature, and anti-tamper
  - Weather, oceanographic and astro-geophysical support needs
  - Transportability and deployability considerations
  - Space, weight, power and cooling margin requirements and open system attributes
  - Derived requirements to support systems that may be used in allied, partner-nation, coalition, or multinational operations relating to U.S.-ratified international standardization agreements
  - Cybersecurity Risk Management for DoD IT Systems
Information Systems (IS)
Information Systems (IS) Development
Streamlining the Requirements Processes

- Sponsors should consider the IS Initial Capabilities Document (IS-ICD) or IS Capability Development Document (IS-CDD) for capability requirements likely to be addressed by IS solutions, software development, and off-the-shelf hardware.

- IS-ICDs and IS-CDDs are variants of regular ICDs and CDDs, implementing the “IT Box” construct.
  - Both streamline the requirements process by delegating oversight and formats for subsequent documents to a flag-level organization other than the JROC or JCB.
    - Provides IS programs greater flexibility to incorporate evolving technologies and achieve faster acquisition.
  - No return to the JROC unless new core capabilities added to the IS-ICD/IS-CDD
Further definition of capabilities through Requirements Definition Packages (RDPs)/Capability Drops (CDs)

Requirements Organization & Oversight
Flag-level oversight [describe oversight body]
- Chair
- Members (list)

IS-ICD
Capability Requirements & Initial Minimum Values
List & Describe Capability Requirements = initial minimum values

IS-CDD
Key Performance Parameters & Initial Minimum Values
List & Describe KPPs = initial minimum values

JROC
Approved IS-ICD or IS-CDD

Hardware Refresh, System Enhancements & Integration Cost Controls
Per year = $XXX
Lifecycle cost = $XXX
Rationale

Application & System Software Development Cost Controls
Per year = $XXX
Lifecycle cost = $XXX
Rationale

• Further definition of capabilities through Requirements Definition Packages (RDPs)/Capability Drops (CDs)

See notes page for more information
Initial Minimum Values

- The IT Box model uses initial minimum values in place of initial objective values so that the baseline capability is clearly specified, and the delegated oversight body has flexibility to further develop capabilities without revalidation of the capability requirements document.
- Initial minimum values represent the achievable level of required capability needed to incorporate current technology to meet the baseline capability.
Applicability of the IT Box

- **IT Box Applies to:**
  - Information Systems (IS) with software development only
  - Includes integration onto commercial off-the-shelf hardware
  - Program costs that exceed $15 million

- **IT Box DOES NOT Apply to:**
  - IS with a developmental cost less than $15 million
  - Defense Business Systems (DBS) (see DoDI 5000.75)
  - Hardware development efforts or capturing capability requirements which span a broad scope of combined hardware, software, and/or DOTmLPF-P efforts.
Information System ICD (IS-ICD)

- IS-ICDs are *Specifically Appropriate* for:
  - Capability requirements when a Capabilities-Based Assessment (CBA) or other study results clearly state that an IS solution is the only viable approach to be considered.
  - Procurement or modification of GOTS/COTS IS products is from domestic or international sources, or the development of dual-use technologies.
  - Additional production or modification of developed DoD, allied, partner-nation, or other U.S. Government agency IS products.
  - Development, integration, and acquisition of customized application software
  - Development of both offensive and defensive cyber capability that meet the remaining criteria for an IS-ICD and require the flexibility that the IT process provides.
  - Approaches where the solution involves research and development and / or acquisition of applications systems software, and the projected life-cycle costs exceed $15 million
- Associated hardware must be COTS/GOTS
- Capability Development Documents (CDDs) are not required as successor documents for an IS-ICD – the delegated authority may prescribe alternate document formats
When an IS-ICD Is Not Appropriate

IS-ICDs are **NOT Appropriate** for:

- Software embedded in a capability solution developed under other validated capability requirement documents.
  - Software requirements are validated as part of the overall capability solution
- Software requiring a host platform, such as a manned or unmanned vehicle, which does not yet have validated capability requirement documents.
  - Software requirements can be included in the capability requirements of the host platform, or as a separate IS-ICD submitted after validation of the host platform capability requirement documents.
- Increases in quantities of previously fielded IS without modification, which are not addressed by an IT Box.
  - Increased quantities may be addressed by a DCR
- Requirements for Defense Business System (DBS) capabilities
IT Box Components for IS-ICD

**Organization & Oversight**
Flag-level oversight through (describe/list) Chair & Members

**Capability Requirements & Initial Minimum Values**
- Capability Requirement 1 [Describe] = Initial minimum value
- Capability Requirement 2 [Describe] = Initial minimum value
- Capability Requirement N [Describe] = Initial minimum value

*(include Net Ready Performance Attribute)*

**“Boundaries”**
JROC-Approved
IS-ICD

[Topic Name]

Oversight Organization [name]
Execution Organization [name]

**Hardware Refresh, System Enhancements, & Integration Cost Controls**
- Per year = $xxx
- Life cycle cost = $xxx
- Rationale

**Application & System**

**Software Development Cost Controls**
- Per year = $xxx
- Life cycle cost = $xxx
- Rationale
Information Systems CDD (IS-CDD)

• IS-CDD
  – Implements IT Box model; **but is not a follow-on to an IS-ICD**
  – Performance attributes (KPPs, KSAs and APAs) may be quantified in terms of initial minimum values rather than threshold/objective values.
  – IS-CDDs streamline the requirements process by delegating oversight and formats for subsequent documents as identified in the IS-CDD.
  – IS-CDDs are appropriate in the same situations where the IS-ICD is appropriate, and are NOT appropriate in the same situations where the IS-ICD is not appropriate.

• In cases where the potential for use of the “IT Box” construct is unclear or in dispute, the Joint Staff Gatekeeper, in consultation with the validation authority as needed, will determine whether an CDD or IS-CDD will be used.

• The validation authority may prescribe appropriate successor documents.

See notes page for more information
IT Box Components for IS-CDD

**Organization & Oversight**
Flag-level oversight through (describe/list) Chair & Members

**Key Performance Parameters & Initial Minimum Values**
List/Describe KPPs = Initial Minimum Values
(include Net Ready Performance Attribute)

**“Boundaries”**
JROC-Approved IS-CDD
[Topic Name]
Oversight Organization [name]
Execution Organization [name]

**Hardware Refresh, System Enhancements, & Integration Cost Controls**
- Per year = $xxx
- Life cycle cost = $xxx
- Rationale

**Software Development Cost Controls**
- Per year = $xxx
- Life cycle cost = $xxx
- Rationale

**Application & System**

**Mandatory KPPs.** Only two of the four mandatory KPPs apply to an IS-CDD: The System Survivability (SS) KPP and Sustainment KPP.
Key Difference In Usage: IS-ICD & IS-CDD

• Key difference in usage of IS-ICDs and IS-CDDs is whether the Analysis of Alternatives (AoA) takes place before or after delegating authorities under the IT Box.
  – For an IS-ICD to be appropriate, it must be very clear from the CBA or other study that an IS solution is the only viable approach to be considered.
  – The AoA conducted in the Materiel Solutions Analysis (MSA) phase takes place after delegating authorities under the IT Box and will therefore only consider IS alternatives.

• An IS-CDD is more appropriate when an IS solution is not presumed at the time the ICD is validated and the Materiel Development Decision (MDD) approved, or other materiel and/or non-materiel solution(s) are expected to be necessary along with the IS solution.
  – The IS-CDD is a result of the AoA conducted in the MSA phase and represents an IS solution for part or all of the capability requirements validated in the ICD.
JCIDS Manual provides the following examples of potential IS-ICD/IS-CDD follow-on documents (actual names, content, and approval determined by the delegated validation authority):

- **Requirements Definition Package (RDP)** or equivalent) is a first level refinement of one or more capability requirements identified in an IS-ICD or IS-CDD, and is co-developed by the operational user (or representative) and the program office – identifies KPPs, KSAs, and APAs, and non-materiel changes.

- **Capability Drop (CD)** (or equivalent) describes the performance characteristics of a relatively small increment of a capability solution included in a software build necessary for partial deployment of the overall capability solution, typically developed and fielded within a short period of time.
  - Could be developed through a rapid prototyping effort with the user to ensure it meets their needs.
  - Commonly, multiple CDs would be derived from a RDP, or IS-CDD.
Requirements Definition Packages (RDPs)

- **RDP is an example** – *It Is Not a JCIDS Document; It identifies performance attributes, it does not contain software specs*
  - Created to show how requirements can be broken into deliverable increments
  - Components define content and approval process
- **Provides a more detailed definition of capabilities in the IS-ICD**
  - Enables detailed design activity
  - Enables detailed costing of the requirements
- **Provides link between the IS-ICD and the acquisition and program budget processes**
- **Approved by the delegated requirements management authority**
  - FO/GO-level body that holds authority over, and provides governance for requirements

See notes page for more information
• CD is an Example – *It Is Not a JCIDS Document; It describes performance characteristics, it does not contain software specs*
  
  – Manages delivery of capabilities through more specifically defined subsets of an RDP
  
  – The details of how to do this are left to the components and the acquisition process

• The RDP is further broken down into CDs to deliver individual “Widgets” or “Slices” of capability

• The results of CD development are released incrementally through full deployment decisions as they are ready

• Approval may delegated to lowest appropriate level (as determined by the oversight authority) to ensure timely decision making

See notes page for more information
This example of RDPs and CDs for managing follow-on efforts is illustrative and is not intended to limit potential flexibility provided by the IS-ICD and IS-CDD.

Actual names, content, approval process and implementation guidance are at the discretion of the delegated oversight authority.

Adapted from Figure A-5, JCIDS Manual, 31 August 2018
Intelligence
Supportability
Intelligence Certification

**Applicability.** All capability requirements documents assigned a JSD of JROC Interest or JCB Interest.

**Objective.** Ensure that capability solutions are developed in the context of applicable adversary threat capabilities, that intelligence requirements have been identified and documented at the earliest possible point, and that all likely intelligence support requirements and shortfalls (if applicable) have been assessed for availability, suitability, and sufficiency.

**Intelligence certification seeks to:**
- Ensure Sponsors incorporate the most current, applicable intelligence information, and analysis into their capability development efforts.
- Ensure that national and defense intelligence architectures remain capable of supporting future warfighting by identifying and assessing possible intelligence support requirement shortfalls created by programs and capabilities being reviewed. Programs that send, produce and/or receive intelligence data and/or services will conform to mandated standards cited in the DoD IT Standards Registry (DISR) and identified by the Functional Managers.
- Preclude fielding capabilities, systems, or programs that are unsupportable by the national and defense intelligence communities.

**Proponent.** J-283/IRCO on behalf of JS/J-2
Critical Intelligence Parameters (CIPs)

• CIPs are defined as a threat capability or threshold established collaboratively by the requirements sponsor and the component capability developer, changes to which could critically impact the effectiveness and survivability of the proposed system.

• CIPs will be included for capabilities in development that are determined to be threat-sensitive.
  - Sponsors should coordinate with DIA during the development of the requirement to determine whether the capability is threat-sensitive and/or if CIPs are required.
  - If DIA determines that a CIP is warranted, they will submit a comment and supporting rationale during JCIDS staffing for Sponsor adjudication.
  - If a CIP is required, the threat validation authority (DIA or Service, as appropriate) will approve the CIP and the Sponsor will ensure the CIP is submitted via the Community On-Line Intelligence System for End Users and Managers (COLISEUM).

• Intelligence certification will be withheld for new or revised programs that do not include a CIP in the JCIDS document during FCB Draft review.
Intelligence Supportability Requirements in ICDs & CDDs

• **ICD Content.** In addition to the requirements for Threat Summary and CIP information, Sponsors must identify the intelligence support categories, when known, applicable to the capability described below in the Capability Requirements and Gaps/Overlays section in ICDs.

  ➢ Include a description of the intelligence support requirements, resources, or other programs necessary to enable each capability, and any current or projected gaps or shortfalls in intelligence support related to a category.

• **CDD Content.** The intent of the intelligence supportability paragraph is to identify and assess all intelligence support requirements, and anticipated shortfalls, throughout the capability solution’s lifecycle in one, comprehensive section of the CDD.
Intelligence Support Category Requirements

• The CDD Intelligence Supportability section must identify and address support requirements, potential shortfalls, and efforts to satisfy shortfalls, or state there are no requirements, for all the intelligence supportability categories below.
  - Intelligence Manpower Support
  - Intelligence Funding Support
  - Intelligence Planning and Operations Support
  - Intelligence Interoperability
  - Targeting Support
  - Intelligence Mission Data Support
  - Space Intelligence Support
  - Counterintelligence Support
  - Intelligence Training Support

Each of these categories are described in detail in the JCIDS Manual Intelligence Supportability Guide.
DOTmLPF-P

Content
• **Applicability.** Sponsors must address all DOTmLPF-P considerations in capability requirements documents.

• In cases where one or more of the DOTmLPF-P considerations may not be applicable, the Sponsor shall state this in the document, explain why, and coordinate with the Joint Staff proponent to ensure that the DOTmLPF-P endorsement is not withheld due to missing information.

• An ICD or DCR should describe non-materiel approaches that could provide a capability solution which closes or mitigates associated capability gaps.

• A CDD should describe non-materiel enablers to materiel capability solutions without which the materiel capability solution cannot be successfully fielded.

• Joint DOTmLPF-P Functional Process Owners (FPOs) (see Figure B-25, JCIDS Manual). The FPOs are subject matter experts within the Joint Staff who provide advice to Sponsors on joint requirement documents and affected FCBs during the staffing and review process.

• **Proponent.** J-7/JCIDS Integration Branch (JIB)
• **Doctrine.** Fundamental principles that guide the employment of U.S. military forces in coordinated action toward a common objective.

• **Organization.** Joint unit or element with varied functions enabled by a structure through which individuals cooperate systematically to accomplish a common mission and directly provide or support joint warfighting capabilities.

• **Training.** Training (including mission rehearsals) of individuals, units, and staffs using joint doctrine or tactics, techniques, and procedures to prepare joint forces or joint staffs to respond to strategic, operational, or tactical requirements considered necessary by the CCMDs to execute their assigned or anticipated missions.

• **materiel.** “materiel” items, systems, or equipment needed to support the required capability. “Little m” materiel refers to increased quantities, modifications, improvements, or alternate applications of existing materiel or the purchase of COTS/GOTS/NDI.

• **Leadership and education.** Professional development of joint leaders that is the product of a learning continuum that comprises training, experience, education, and self-improvement.
• **Personnel.** Ensures that qualified personnel exist to support joint capability requirements. The DOTmLPF-P personnel function should not be confused with the organization function. The number or quantity of personnel is a function of organization, while the quality, type, or skills of personnel is considered in the personnel function.

• **Facilities.** Real property consisting of one or more of the following: buildings, structures, ranges, utility systems, associated roads and other pavements, and underlying land. Key facilities are defined as command installations and industrial facilities of primary importance to the support of military operations or military production programs.

• **Policy.** Any DoD, interagency or international policy issues that may impact effective implementation of changes in the other DOTmLPF-P considerations.
Weapons Safety Assurance
Weapons Safety Assurance

- **Applicability.** Munitions as defined in Title 10 U.S.C. § 101*. Also, directed energy weapons (DEW), EM rail guns, and all firing, launching, safety critical software, and controlling systems as part of the definition.
  - Exceptions include nuclear weapons and their components; small arms and associated ammunition not containing electronics or software; intercontinental ballistic missiles; and space launch vehicles.

- Because all weapons/weapons systems have the potential of being deployed together or employed in joint environments, weapons and weapons systems will be considered joint systems within the JCIDS process and may be designated as JROC or JCB Interest.

- If tailoring of one or more safety requirements is proposed, the CDD weapon safety assurance section shall provide the weapon safety requirements which deviate from the standards, with rationale for the deviations, traceable to the joint or multinational mission environment, and the attributes and performance parameters that must be met as the basis for increased or decreased weapon safety requirements.

- **Proponent.** Protection FCB

*All ammunition products and components produced for or used by the armed forces for national defense and security, including ammunition products or components under the control of the Department of Defense, the Coast Guard, the Department of Energy, and the National Guard.
Baseline Weapons Safety Requirements

• **System Safety.** Sponsors will identify the acceptable risk levels for weapon safety assurance IAW DoDI 5000.02. System safety and acceptable risk requirements informs the development of a System Safety Program (SSP) for the lifecycle of the weapon system IAW DoDD 5000.01 and MIL-STD-882E.

• **Insensitive Munitions (IM).** Standardized IM test protocols used in assessing a weapon’s response to unplanned threats are established in JROCM 235-06 and MIL-STD-2105D.

• **Fuse Safety.** Fuse safety requirements are established in MIL-STD-1316F, Joint Ordnance Test Procedures 051 and 052.

• **Explosive Ordnance Disposal (EOD).** Requirements for disposal of munitions containing or delivering energetic materiel must satisfy the EOD RDT&E authority IAW DoDD 5160.62. Requirements for disposal will inform the development of a demilitarization and disposal plan.

• **Laser Safety.** If the munitions contain lasers, to protect and mitigate the risk to personnel from laser radiation to an acceptable level, requirements for engineering design, protective equipment, administrative controls, or a combination thereof are established in DoDI 6055.15.
Baseline Weapons Safety Requirements
continued..

- **E3 Ordnance Safety.** E3 ordnance safety requirements are established in MIL-STD-464C and MIL-STD-464G, including but not limited to hazards of electromagnetic radiation to ordnance, electrostatic discharge, EMP, electromagnetic interference, electromagnetic vulnerability, lightning, and precipitation-static.

- **Weapon Packing, Handling, Storage, and Transportation.** Safety standards for packing, handling, storage, and transportation are established in DODM 6055.09 (Vol 1 – 8).

- **Other Considerations.** In addition to criteria in the categories above, Sponsors should consider criteria shown in Figure B-27, JCID Manual.
JCIDS Document
Staffing and Validation
JCIDS Gatekeeper

• J-8, Deputy Director for Requirements and Capability Development (DDRCDD) is the Gatekeeper

• The Gatekeeper:
  - Performs an initial review of all JCIDS proposals
  - Gatekeeper determines:
    - Joint Staffing Designator (JSD)
      - JROC Interest
      - JCB Interest
      - Joint Information
    - Lead and supporting Functional Capability Boards (FCBs)

• Formal staffing begins after gatekeeper decisions
Joint Staffing Designator (JSD)
JROC Interest

- **JROC Interest**
  - Capability requirements documents that have performance attributes considered critical or essential to ensure joint interoperability and are necessary to fulfill a capability gap(s) of more than one armed force, agency or entity of the DoD.
  - JROC Interest is used for documents where the intended level of joint oversight cannot be satisfied by assignment of a lower level JSD.
  - JROC Interest capability requirements documents will have at least one JPR where the capability requirement has clear joint interoperability or multi-service equities.
  - The JROC is the validation authority for JROC Interest documents.

All capabilities, regardless of JSD, should consider interoperability within the joint force to include joint force enablers.
Joint Staffing Designator (JSD)

JCB Interest

- Capability requirements documents that have performance attributes considered critical or essential to ensure joint interoperability and are necessary to fulfill a capability gap(s) of more than one armed force, agency or entity of the DoD.

- Capability requirements documents where the intended level of oversight does not meet the JROC threshold and cannot be satisfied by assignment of a lower level JSD.

- The JCB is the validation authority for JROC Interest documents, except that US Special Operations Command (USSOCOM) and US Cyber Command (USCYBERCOM) have independent validation authority for JCB Interest and below documents.

- JCB Interest is the minimum JSD for Joint DCRs and for any documents where the Sponsor is a CCMD, with the exception of USSOCOM or USCYBERCOM.

- JCB Interest capability requirements documents will have at least one JPR where the capability requirements has clear interoperability or multi-service equities.

See notes page for more information.
• **Joint Information**
  
  – Capability requirements documents that do not need Joint Staff certifications or endorsements and are below the level of JCB Interest.
  
  – The Sponsor organization has independent validation authority for Joint Information documents and responsibility for applicable certifications and endorsements. Any applicable waivers will be published for visibility.
  
  – The Service Gatekeeper will be responsible for ensuring timely communication with the Joint Staff Gatekeeper regarding the status of the document and will provide the Joint Staff Gatekeeper a copy of the validated capability requirements document and associated validation memorandum when complete.
### Certification or Endorsement Authority

<table>
<thead>
<tr>
<th>Certifications &amp; Endorsements</th>
<th>JROC/Interest or Joint Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net Ready Certification</td>
<td>Sponsor (or Joint Staff if designated a JPR)</td>
</tr>
<tr>
<td>Force Protection KPP Certification</td>
<td>Sponsor (or Joint Staff if designated a JPR)</td>
</tr>
<tr>
<td>System Survivability KPP Endorsement</td>
<td>Sponsor (or Joint Staff if designated a JPR)</td>
</tr>
<tr>
<td>Sustainment KPP Endorsement</td>
<td>Sponsor (or Joint Staff if designated a JPR)</td>
</tr>
<tr>
<td>Energy KPP Endorsement</td>
<td>Sponsor (or Joint Staff if designated a JPR)</td>
</tr>
<tr>
<td>DOTmLPF-P Endorsement</td>
<td>Joint Staff (delegated to Sponsor for Joint Information Documents)</td>
</tr>
<tr>
<td>Threat Assessment/Intelligence Certification</td>
<td>Joint Staff (delegated to Sponsor for Joint Information Documents)</td>
</tr>
<tr>
<td>Weapon Safety Endorsement</td>
<td>Joint Staff (only applicable to JROC/JCB Interest)</td>
</tr>
</tbody>
</table>

- Sponsors have certification and endorsement authority for all performance attributes which are not JPRs. The Joint Staff has certification and endorsement authority for all JPRs.
- USSOCOM and USCYBERCOM have certification and endorsement authority for all JPRs in capability requirements documents with a JSD of JCB Interest or below.
JROC Decision Chain

- **JROC: Joint Requirements Oversight Council**
- **JCB: Joint Capability Board**
- **FCB: Functional Capability Board**
- **FCB WG: Functional Capability Board Working Group**

JROC Membership

Chair: VCJCS

Council Members:
- Vice Chief of Staff, Army
- Vice Chief of Naval Operations
- Vice Chief of Staff, Air Force
- Assistant Commandant of the Marine Corps

Advisors to the JROC:
- USD(A&S), USD(R&E), USD(Intel), USD(Comptroller), USD(P), USD(P&R), DoD CIO, Dir. CAPE, and DOT&E.

Commander of a combatant command when matters related to the area of responsibility or functions of that command are under consideration.
The JROC is the highest-level board and JCIDS owner. The JROC assists CJCS in:

- Assessing joint military capabilities, and identifying, approving, and prioritizing gaps in such capabilities, to meet applicable requirements in the National Defense Strategy (NDS);
- Reviewing and validating whether a capability proposed by an Armed Force, Defense Agency, or other entity of the DoD fulfills a gap in joint military capabilities;
- Establishing and approving joint performance requirements;
- Reviewing performance requirements for any existing or proposed capability that the CJCS determines should be reviewed by the JROC;
- Identifying new joint military capabilities based on advances in technology and concepts of operation; and
- Identifying alternatives to any acquisition program that meets approved joint military capability requirements.

See notes page for more information
Joint Capabilities Board (JCB)

• One level below the JROC.
• Provides review and endorsement of documents and adjudication of lower level issues prior to JROC validation
• Validates JCIDS documents with a Joint Staffing Designation (JSD) of “JCB Interest”, except JCB Interest documents under USSOCOM and USCYBERCOM.
• Nominates topics for JROC consideration and advises on issues requiring JROC review.
• JCB Chair: Director, J-8
• JCB Membership: General/Flag Officers, or civilian equivalent, from the military services.

See notes page for more information
Functional Capabilities Boards (FCBs)

• One level below the JCB.
• Provides capability requirement portfolio management, including review and assessment of documents and adjudication of lower level issues within their portfolio prior to JCB review
• Participates in Joint Concept Development activities
• Nominates topics for JROC or JCB consideration and advises on issues requiring JROC or JCB review.
• Coordinates with USD(R&E) and/or USD(A&S) to obtain the current status of the development of any Joint area mission-based inputs in the requirements process
• Aligned with Joint Capability Areas (JCAs)
• FCB Chair: General/Flag Officer, or Civilian Equivalent
• FCB Membership: Representatives in military grade of 0-6, or civilian equivalent, from Joint Staff, Services, CCMDs, and other DoD organizations with equity in the FCB’s portfolio

See notes page for more information
JCA 8, Corporate Management, does not have a FCB. Corporate Management issues related to Defense Business Systems are managed by the Chief Management Officer, along with common gatekeeping processes with JCIDS via the Joint Staff Gatekeeper. Other Corporate Management issues will be handled through one of the listed FCBs with appropriate participation from other organizations.
Functional Capabilities Board Working Groups (WGs)

- One level below the FCBs
- Provide initial review and assessment of documents and issues prior to review by the FCB
- Participate in Joint Concept Development activities
- Established by the FCB Chair
- FCB WG Lead: Military Officer, 0-6, or Civilian Equivalent
- FCB WG Membership: Military, civilian, or contractor support Subject Matter Experts from Joint Staff, Services, Combatant Commands, and other organizations with equity in the FCB’s portfolio.
Other Related Organizations

• In addition to the Gatekeeper, there are several organizations that participate directly with the four levels of boards (JROC, JCB, FCB and FCB WG):
  – Independent Assessment Organizations Within J-8
    ➢ J-8 / Joint Requirements Assessment Division
    ➢ J-8 / Capabilities and Acquisition Division
    ➢ J-8 / Program and Budget Analysis Division
  – FCB General Officer / Flag Officer (GO/FO) Integration Group
  – FCB 06 Integration Group
  – Joint Weapon Safety Technical Advisory Panel
  – Document Sponsor
  – Milestone Decision Authority
The deliberate staffing process begins when the Joint Staff Gatekeeper, after screening and review, submits the document into JCIDS.
The deliberate staffing process begins when the Joint Staff Gatekeeper, after screening and review, submits the document into JCIDS.

See notes page for more information.
Summary of the Deliberate JCIDS Process

- **Materiel Solutions**
  - Initial Capabilities Document (ICD) and IS Variant (IS-ICD)
  - Capability Development Document (CDD) and IS Variant (IS-CDD)

- **Non-Materiel Solutions** – Joint DOTmLPF-P Change Request (DCR)

- **Operational requirements development** is a team effort; all stakeholders should be involved; involve the user in technical requirements development
Urgent Needs
Urgent Need Situations

• Urgent and compelling needs during crisis and conflict, or anticipated or pending contingency operation

• Each Military Service has policies and procedures, but ...
  
  ➢ Service-unique approaches do not address theater-wide Joint Urgent and Joint Emergent Operational Needs
  
  ➢ Requirements Managers need to stay engaged in the process

The Warfighter Senior Integration Group (SIG) is the Oversight Body for DoD Urgent Needs
See DoDD 5000.71, 24 Aug 2012
## Urgent & Emergent Threat Lanes

<table>
<thead>
<tr>
<th>JCIDS Lanes</th>
<th>Operational Timeline</th>
<th>JCIDS Documents</th>
<th>JCIDS Staffing Timeline</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ongoing Contingency Lane</strong></td>
<td>Urgent Need (&lt;2 Years)</td>
<td>JUON</td>
<td>15 days</td>
</tr>
<tr>
<td><strong>Anticipated Contingency Lane</strong></td>
<td>Emergent Need (&lt;2Years)</td>
<td>JEON</td>
<td>31 days</td>
</tr>
<tr>
<td><strong>Deliberate Lane</strong></td>
<td>Future Need (&gt;2Years)</td>
<td>ICD</td>
<td>97 days</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CDD</td>
<td>103 days</td>
</tr>
</tbody>
</table>

The Ongoing Contingency Lane is the **Joint Urgent Operational Needs (JUON) Lane**

The Anticipated Contingency Lane is the **Joint Emergent Operational Needs (JEON) Lane**
• **Urgent Operational Need (UON):**
  – Capability requirements identified by a DOD Component as impacting an ongoing or anticipated contingency operation. If left unfulfilled, UONs result in capability gaps potentially resulting in loss of life or critical mission failure. DoD Components, in their own terminology, may use a different name for a UON.

• **Joint Urgent Operational Need (JUON):**
  – UONs that are identified by a Combatant Command (CCMD) as inherently joint and impacting an ongoing contingency operation.

• **Joint Emergent Operational Need (JEON):**
  – UONs that are identified by a CCMD as inherently joint and impacting an anticipated or pending contingency operation.
Who Initiates a JUON or JEON?

• **JUONS or JEONS are submitted by CCMDs or the CJCS/VCJCS**
  
  – While JUONs and JEONs are primarily submitted by the CCMDs, the CJCS/VCJCS may generate a JUON or JEON directly in support of CJCS or VCJCS responsibilities, or to facilitate timely validation of urgent or emergent needs identified by multiple CCMDs or DOD Components.
  
  – Submitted by SIPRNET email or memo to the Joint Staff Gatekeeper

• **New JUONs or JEONs, and modifications to requirements in validated JUONs or JEONs, must be endorsed by the CCMD Commander, Deputy Commander, or Chief of Staff.**
  
  – Administrative modifications to previously validated JUONs or JEONs may be endorsed by the CCMD J8.
Use & Purpose of UONs

• **Use.** JUONs, JEONs, and Component UONs are used ONLY when there are urgent requirements for capabilities that do not exist in the joint force, and where the deliberate requirement acquisition processes, or other means such as the Global Force Management (GFM) process, Joint Manpower Validation Process (JMVP), etc., are not practical for satisfying the capability requirements in the operational timelines.

  – JUONs and JEONs support urgent and emergent capabilities associated with on-going and anticipated contingency operations; and as such, Sponsors should field an initial capability solution in less than 2 years.

• **Purpose.** JUONs, JEONs, and Component UONs facilitate rapid identification, prioritization, validation, documentation, and communication of urgent or emergent capability requirements and associated capability gaps that represent significant risk to mission success or safety of forces.

  – These documents serve as the basis for expedited validation by the validation authority and rapid acquisition of materiel solutions.
DoD Component UONs are reviewed and validated by DoD Component processes.

Goal for staffing and validation of JUONs is 15 days; JEONS is 31 days.

JUON or JEON validation and resourcing involves:

- J8 Deputy Director for Requirements & Capability Development (DDRCD) validates JUONs.
- JCB or JROC validates JEONs as determined by VCJCS.
- Collaborative review by the Lead FCB and the Joint Rapid Acquisition Cell (JRAC) identifies potential solution approaches (COTS, GOTS, NDI, acceleration of ongoing acquisition program or S&T efforts).
- Solution Sponsor (normally a military department) designated by the JRAC funds, develops, acquires, fields and sustains the solution – may require out-of-cycle funding.
The Requirements Sponsor provides the JUON to the Joint Staff Gatekeeper and to the Director, JRAC for initial screening and review. Staffing begins when the Gatekeeper submits the document from the Requirements Sponsor into JCIDS.

The diagram illustrates the process:

1. **JUON Staffing (15 days)**

   - **Sponsor**: JUON
   - **Gatekeeper**
   - **FCB**: Accept & Assign JCD?
     - Yes: FCB Review
     - No: Revise Document
   - **DDRCD**: Validate Joint Military Capability Requirement?
     - Yes: JROCM
     - No: NO

   - Time:
     - 1 day
     - 14 days

See notes page for more information.
The Requirements Sponsor provides the JEON to the Joint Staff Gatekeeper and to the Director, JRAC for initial screening and review. Staffing begins when the Gatekeeper submits the document from the Requirements Sponsor into JCIDS.
Urgent/Emergent Path & Urgent Acquisition Process

Interaction of JCIDS Urgent/Emergent Path and Urgent Capability Acquisition Process
JUON & JEON Validation Reviews

• Quarterly Review.
  – The Joint Staff Gatekeeper, together with the JRAC, reviews validated JUONs and JEONs quarterly to assess progress toward fielding capability solutions in a timely manner. Similar reviews at Component level for Component UONs. Results are briefed to the Warfighter SIG.

• Assessment of Operational Utility
  – The original requirement Sponsor will generate an assessment of the capability solution no later than six months after initial delivery to facilitate transition, sustainment, or alternate approaches.

• Biannual Review.
  – Unless withdrawn earlier by the validation authority or requirement Sponsor, the validation authority reviews validated JUONs and JEONs two years after the validation date.
The three categories for the conclusion in the Operational Utility Assessment are:

• **Failure/Limited Success.**
  – The fielded solution does not provide operational utility satisfying the capability requirements in the validated JUON or JEON. The Requirements Sponsor provides confirmation that the originally requested and validated capability requirements are still appropriate or identifies any necessary changes for revalidation.

• **Success/Limited Duration Requirement.**
  – The capability solution satisfies the urgent/emergent capability requirement for the limited duration purposes identified in the validated JUON or JEON.

• **Success/Enduring Requirement.**
  – The capability solution satisfies the urgent/emergent capability requirement for the limited duration purposes identified in the validated JUON or JEON, but also provides enduring capabilities that should remain in the joint force.
Assessments recommending enduring capability requirements will be endorsed by the original authorizing official (CCMD Commander, Deputy Commander, or Chief of Staff), reviewed by the FCB WG or FCB, and validated by the appropriate validation authority.

The FCB may recommend to the validation authority for transition to an enduring capability requirement even when the original authorizing official does not recommend it.

Once determined that the transition will happen, the Requirements Sponsor will consider the need to generate a CDD, DCR, or other appropriate documentation for validation to identify the performance attributes, DOTmLPF-P considerations, and supporting information for the balance of development, fielding, and required sustainment to meet the follow-on enduring capability solution.
Transition to Program of Record (PoR)

• Who decides if a solution to an Urgent Operational Need must enter the formal acquisition process?
  – ACAT ID – Defense Acquisition Executive (DAE)
  – ACAT IB, II or below – Component Acquisition Executive (CAE) / Service Acquisition Executive (SAE)

• May need Materiel Development Decision (MDD) depending on:
  – Status of procurement
  – If the fielded solution needs additional development

• Funding for additional quantities and sustainment is Service responsibility
Challenge of Rapid Acquisition

Future Focused
Very Structured Process
Evolved Requirements
Analysis of Alternatives
Lengthy Development
High Visibility on Program
Large Investment

Now-focused
More ad hoc process
Broad requirement
Quick assessment of alternatives
Limited development
High visibility on results
Limited investment
Very Limited Feedback
Transition to PoR
Urgent Operational Need Summary

• An urgent / emergent situation that may result in
  – Loss of life and/or
  – Critical mission failure

• Each service has its own approach to urgent needs that are not joint

• JUONs / JEONs document joint urgent needs

• Requirements Managers need to be involved with follow-on activities
Guiding Principles

• **Know the requirements**—the requirements/acquisition community should not only clearly understand the requirements, but should be actively engaged with the user in establishing realistic and achievable requirements within budget constraints.

• **Question the requirements**—if a requirement doesn’t make sense, question it—the answer may be surprising.

• **Are the requirements realistic**—is it physically possible to meet the requirement? Can it be tested? Is an 80% solution adequate and field the remaining 20% when technology is mature enough?

• **Beware of derived requirements**—an engineer’s “derived” technical requirement can take on a life of its own; keep focused on the user’s operational requirements.

• **Tech Reviews**—JCIDS sponsor/user should attend PDR and CDR to answer questions on operational requirements.

• **Configuration Steering Boards (CSBs)**—PM has the authority to recommend descoping options and to object to new requirements after MS B, unless approved by the CSB. Must be coordinated with the requirements professionals.
Requirements Challenges

• Gaming the System by Specifying the Solution too Early
• Incomplete or Rushed Analysis
• Vague/Poorly Written Requirements
• Good Briefings Based on Poor Documents
• Confusing Operational Requirements with Technical Requirements (Specifications)
• Not Following Up on Results of Milestone/Decision Reviews and T&E results
• Requirements Creep (Operational & Technical)
• Misusing the Urgent/Emergent Requirements Determination Processes
• Cost and Schedule Estimates Based on Incomplete or Poorly Written Requirements (Operational and Technical)
Backups
Some Useful JCIDS Terms

- **Capability** - The ability to complete a task or execute a course of action under specified conditions and level of performance.

- **Capability Gap** - The inability to meet or exceed a capability requirement, resulting in an associated operational risk until closed or mitigated.

- **Capability Requirement** - A capability which is needed to meet an organization’s roles, functions, and missions in current or future operations. May also be referred to as a “capability need”, “need”, and/or a “requirement”

- **Capability Requirements document** – Any document used to articulate either deliberate or urgent/emergent capability requirements and associated information pertinent to review and validation.

- **Capability Solution** - A materiel solution or non-materiel solution to satisfy one or more capability requirements and reduce or eliminate one or more capability gaps. Also called, “solution”.

- **Joint** - Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. *Note that this definition of “joint” is applicable to capability requirements documents and capability solutions which apply to more than one DoD Component.*

- **Joint Performance Requirement (JPR)** - A performance requirement that is critical or essential to ensure interoperability or fulfill a capability gap of more than one armed force, Defense Agency, or other entity of the Department of Defense, or impacts the joint force in other ways such as logistics.

- **Sponsor. Document Sponsor** - The organization submitting a capability requirements document. **Solution Sponsors** for successor documents - CDDs and Joint DCRs - may be different from the Requirement Sponsors for initial documents - ICDs, UONs, JUONs, and JEONs. This occurs when the Document Sponsor does not have acquisition authority.
Getting The Front End Right is Key