Defense Information Systems Agency

A Combat Support Agency

Joint Interoperability Test Command

JCIDS Document Review Checklist

Version 1.0, 12 May 2009

for

CDDs, CPDs, ISPs, and TISPs

developed in accordance with

CJCSI 6212.01E, 15 December 2008

Caution: This checklist was developed for the use of JITC Action Officers and support contractors. It is not comprehensive and addresses only areas of JITC concern, e.g. interoperability and net-centricity.

This is a living document and will be update, as required. JITC Action Officers and support contractors should always verify they have the correct version before starting a review.

See: T:\PLANS & POLICIES TRAINING\JCPAT-E document review\nr-kpp document review checklist

Send comments to Alvin Mack or Freddy Haukaas.

JITC Document Review Checklist
CJCSI 6212.01E
Version 1.0, 12 May 2009

X. Requirement X.X Potential Issue(s)	**CDD**[4]	**CPD**[4]	**ISP**[4]	**TISP**[4]	**Maximum Level of Criticality**[5]	**Guidance**	**Reference**[1]
0. Net-Ready Key Performance Parameter (NR-KPP) Compliance Statement							
0.1. Does the document contain the NR-KPP compliance statement?	X	X	X	X	C	The NR-KPP compliance statement is the basis for the IOP certification process and is required for testing.	Encl E, para 1.a DODI 4630.8, para 6.1.3 (ISP) Compliance statement Encl E, page E-21
0.2. Is the NR-KPP compliance statement modified from the standard NR-KPP compliance statement?	X	X	X	X	S	The NR-KPP compliance statement is the basis for the IOP certification process. We must be aware of any modification of the statement. The JS J-6 must approve any modification to the statement.	
1. Solution Architectures https://dars1.army.mil/ (log in required)							
1.1. General							
1.1.1. Do the solution architectures show linkages to parent enterprise architectures, if available?	X	X	X	X	C	Solution architectures that show linkages to parent enterprise architectures support consistency of interoperability testing and certification.	Encl E, para 3.b.(1)(b)
1.1.2. Do the solution architectures fit within Component and DoD Capability Portfolio Management architecture descriptions?	X	X	X	X	C	Solution architectures that fit within Component and DoD Capability Portfolio Management architecture descriptions support consistency of interoperability testing and certification.	Encl E, para 3.b.(1)(b)
1.1.3. Does the system have its TV-1 and TV-2 registered online in DISRonline?	X	X	X	X	S	Online registration of the system's TV-1 and TV-2 provides a common basis for understanding the system. This common understanding results in more accurate interoperability tests and certifications.	Encl E, para 3.b.(1)(g)
1.1.4. Does the document provide a reference to the online TV-1and TV-2?	X	X	X	X	S		Encl E, para 3.b.(1)(g)
1.1.5. Are the solution architectures submitted in data formats that are viewable without specialized or proprietary tools?	X	X	X	X	C	JITC does not possess any special tools to enable review of products in non-specialized tools. The AO should coordinate with the proponent to see if they can provide the architectures.	Encl E, para 3.b.(1)(m)

JITC Document Review Checklist
CJCSI 6212.01E
Version 1.0, 12 May 2009

X. Requirement X.X Potential Issue(s)	**CDD**[4]	**CPD**[4]	**ISP**[4]	**TISP**[4]	**Maximum Level of Criticality**[5]	**Guidance**	**Reference**[1]
1.1.6. Are the solution architectures legible?	X	X	X	X	C	Non-legible architecture products may lead to incorrect interpretations, which could lead to potentially serious problems at test time.	Encl E, para 3.b.(1)(m)
1.1.7. Does the solution architecture support traceability of joint critical operational activities?	X	X	X	X	C	Traceability of joint critical operational activities supports accurate evaluation of testing requirements.	Encl E, para 3.d.(2)
1.2. AV-1: Overview and Summary Information (III)[7]							
1.2.1. Is the AV-1 present?	X	X	X	X	S	The AV-1 provides executive-level summary information in a consistent form that allows quick reference and comparison among architectures. AV-1 includes assumptions, constraints, and limitations that may affect high-level decision processes involving the architecture.	DoDAF, section 3.1
1.2.2. Does the AV-1 provide accurate information?	X	X	X	X	S		
1.2.3. Does the system have its AV-1 registered online in DARS?	X	X	X	X	S	Online registration of the system's AV-1 provides a common basis for understanding the system. This common understanding results in more accurate interoperability tests and certifications.	Encl E, para 3.b.(1)(e)
1.2.4. Does the document provide a reference to the online AV-1?	X	X	X	X	S	Online registration of the system's AV-1 provides a common basis for understanding the system. This common understanding results in more accurate interoperability tests and certifications.	Encl E, para 3.b.(1)(e)
1.3. OV-1: High-Level Operational Concept Graphic (III)[7]							
1.3.1. Is the OV-1 present?	X	X	X	X	S	The OV-1 is the most general of the architecture products. Check for explanatory text. Ensure the OV-1 captures mission and highlights main operational nodes.	DoDAF, section 4.1
1.3.2. Does the OV-1 provide accurate information?	X	X	X	X	S		
1.3.3. Are the organizations, organization types, and/or human roles traceable to the OV-2?	X	X	X	6	C	The OV-1's objects (e.g., organizations and human roles) should trace to the OV-2's nodes. Successful traceability will result in more accurate interoperability testing and certification.	

X. Requirement X.X Potential Issue(s)	**CDD**[4]	**CPD**[4]	**ISP**[4]	**TISP**[4]	**Maximum Level of Criticality**[5]	**Guidance**	**Reference**[1]
1.3.4. Do relationships trace to needlines in the OV-2?	X	X	X	6	S	The OV-1's object relationships (i.e., between organizations and between organizations and human roles) must trace to the OV-2's needlines. The OV-2's needlines provide the OV-1's relationships with specific identification and attributes, which will result in more focused interoperability testing and certification.	
1.4. OV-2: Operational Node Connectivity (II) [7]							
1.4.1. Is the OV-2 present?	X	X	X	6	C	The needline/node identifier is essential to tracing needlines and information exchanges across the other architectural products. A needline is a relation between Operational nodes showing that these two nodes communicate to each other and exchange information. An Operational node is an element that produces, consumes, or manipulates information.	DoDAF, section 4.2
1.4.2. Does the OV-2 include unique needline(s)/node ID(s)?	X	X	X	6	C		
1.4.3. Does the OV-2 provide details on associating an organization type to a node, if needed to understand the facilities/system nodes?	X	X	X	6	S	OV-2 can also group organizational structure elements from OV-4.	
1.4.4. Are the organizations, organization types, human roles and/or needlines traceable to the OV-1?	X	X	X	6	S	The organizations, organization types, human roles and/or needlinesshown in various views must trace back to the OV-1. This will provide consistency of interoperability testing and certification.	
1.4.5.							
1.4.6. Do OV-2 needlines map to one or more information exchanges in OV-3?	X	X	X	6	S	The OV-2's needlines must map to the OV-3's information exchanges. This will provide consistency of interoperability testing and certification.	

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
1.4.7. Do the activities annotating an operational node in an OV-2 map to the activities described in an OV-5?	X	X	X	6	S	The activities annotating OV-2's operational node must map to the corresponding activities described in the OV-5. This will provide consistency of interoperability testing and certification.	
1.4.8. Do the operational nodes in the OV-2 map to lifelines in the OV 6c?	X	X	X	6	S	The OV-2's operational nodes must map to the OV-6c's lifelines. This will provide consistency of interoperability testing and certification.	
1.4.9. Are operational nodes supported by one or more systems in SV-1 (indicating that the operational node owns/uses the system)?	6	6	6	6	S	Each operational node must be supported by one or more systems shown in the OV-1. This will provide completeness of operational node/system relationships within interoperability testing and certification.	
1.4.10. Do needlines map to one or more interfaces in the SV-1?	6	6	6	X	S	The system needlines must map to one or more interfaces in the SV-1. This will provide completeness of needlines within interoperability testing and certification.	
1.5. OV-3 Information Exchanges (I)[7]							
1.5.1. Is the OV-3 present?	X	X	X	X	C	The OV-3 depicts information exchanges between nodes and the relevant attributes of those exchanges Each system information exchange must be associated with at least a pair of nodes and corresponding organizations/users, a needline, and usually, though not always, an interface description (per the SV-1).	DoDAF, section 4.3
1.5.2. Does each information exchange map to a needline in the OV-2?	X	X	X	6	C		
1.5.3. Do OV-3 triggering events map to OV-6c events?	X	X	X	X	C	OV-3 triggering events must map to OV-6c events. This will provide the correct sequence of events.	
1.5.4. Are OV-3 information elements constructed of entities in OV-7?		**2**	**3**		C	OV-3 information elements should correspond to OV-7 elements for structured exchanges. They may not correspond for unstructured exchanges, e.g., voice links or free-text messages.	

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
1.5.5. Do the automated OV-3 information exchanges map to one or more system data exchanges in SV-6?	X	X	X	X	C	Each system data element in SV-6 should map to some information element in the OV-3, but reverse may not be true as levels of abstraction of OV-3 and SV-6 may differ, and information to system data element mapping may be incomplete or ambiguous. Note: The SV-6 contain only automated information exchanges.	
1.6. OV-4: Organizational Relationships Chart (III)[7]							
1.6.1. Is the OV-4 present?	X	X	X	6	S	Many OV-4s are constructed in similar nature to organization charts: dashed lines indicate a supporting role and solid lines indicate directing or commanding role.	DoDAF, section 4.4
1.6.2. Do the nodes depicted in the OV-2 and the relationships depicted in the OV-4 agree?	X	X	X	6	S	You should be able to trace group organizational structure elements from the OV-4 to the OV-2.	
1.7. OV-5: Operational Activity Model (I)[7]							
1.7.1. Is the OV-5 present?	X	X	X	X	C	The OV-5 describes the operations that are normally conducted in the course of achieving a mission or a business capability. It describes capabilities, operational activities (or tasks), input, and output (I/O) flows between activities, and I/O flows to/from activities that are outside the scope of the architecture	DoDAF, section 4.5
1.7.2. Does the OV-5 include required operational nodes/activities?	X	X	X	X	C	The JITC needs to know the input/output flow of the operational nodes/activities.	
1.7.3. Does the OV-5 clearly delineate lines of responsibility in association with OV-2/OV-4?	X	X	X	6	C	The OV-5 must clearly delineate lines of responsibility for activities when coupled with the OV-2 and OV-4.	
1.7.4. Is the OV-5 linkage to the OV-6c clear?	X	X	X	X	C	The OV5 provides a necessary foundation for depicting activity sequencing and timing in OV-6c.	
1.7.5. Can you determine the criticality of the OV-5 activities?	X	X	X	X	C	Critical mission threads and operational information exchanges should be annotated as critical.	

X. Requirement X.X Potential Issue(s)	**CDD**[4]	**CPD**[4]	**ISP**[4]	**TISP**[4]	**Maximum Level of Criticality**[5]	**Guidance**	**Reference**[1]
1.7.6. Do the operational activities depicted in the OV-5 map correctly to the SV-5?	X	X	X	X	C	The OV-5's operational activities must map to the SV-5's operational activities. This will provide consistency in interoperability testing and certification.	
1.7.7. Does the OV-5 include discussion or representation of any constraints and/or does the operational logic appear to be consistent with the other architectural products?	X	X	X	X	S	The OV-5 should define the flow of the operational activities.	
1.7.8. Does the OV-5 document the OV-2 operational nodes that participate in each operational activity?	X	X	X	6	S	The OV-5 must document the OV-2's operational nodes that participate in each operational activity. This will provide consistency in interoperability testing and certification.	
1.7.9. Do inputs and outputs of operational activities map to OV-6c events?	X	X	X	X	S	The inputs and outputs of the OV-5's operational activities must map to the OV-6's events. This will provide consistency in interoperability testing and certification.	
1.7.10. .If program/system is a producer and/or consumer of NCES; does the OV-5 identify net-centric activities?	X	X	X	X	C	The OV-5 will reflect participation in the DoD enterprise discovery processes. In the Net Centric Environment, the OV-5 should capture the capabilities, activities, and information flows for posting information and data.	
1.8. OV-6c: Operational Event-Trace Description (II) [7]							
1.8.1. Is the OV-6c present?	X	X	X	X	C	Multiple OV-6cs are common. They may document non-automated operational activity sequences or scenarios. Exchanges are documented in OV-3 and SV-6.	DoDAF, section 4.6
1.8.2. Does the OV-6c provide sequence of operational events?	X	X	X	X	C	The OV-6c should define the timing and sequence of messaging events across multiple operational nodes (depicted as swim lanes)	
1.8.3. Does the OV-6c provide timeliness information?	X	X	X	X	S	The OV-6c should identify the warfighters timeliness requirement from an end-to-end perspective. Timeliness data may not be ready for a CDD.	

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
1.8.4. Do OV-6c lifelines map to OV-2 operational nodes?	X	X	X	X	S	The OV-6c's lifelines must map to the OV-2's operational nodes. This will provide consistency in interoperability testing and certification.	
1.8.5. Do OV-6c events map to OV-3 triggering events?	X	X	X	X	S	The OV-6c's events must map to the OV-3's triggering events. This will provide consistent scenarios in interoperability testing and certification.	
1.8.6. Do OV-6c events map to OV-5 inputs and outputs of operational activities?	X	X	X	X	S	The OV-6c's events must map to the OV-5's inputs and outputs of operational activities. This will provide consistency in interoperability testing and certification.	
1.8.7. Do any capabilities associated with a specific sequence in OV-6c match a system, function, or service documented in SV-5a/b/c?	X	X	X	X	S	Any system, system function, or service documented in the SV-5a/b/c must map to an operational node in one or more OV-6cs. This will provide consistency in interoperability testing and certification.	
1.9. OV-7: Logical Data Model (I) [7]							
1.9.1. Is the OV-7 present?		**2**	**3**		C	The Logical Data Model is only required to depict/describe two data elements: entity type and relationship type along with their respective attributes. CPDs will include the Logical Data Model (OV-7) if the system being described collects, processes, or uses any shared data not prescribed by NCES or KIP use (includes database systems).	DoDAF, section 4.7
1.9.2. Are all input/output entities represented in the OV-7?		**2**	**3**		S	The OV-7 reflects the structure and flow of key information. The content of this product should be directly attributable to the input/output entities identified during construction of the OV-6c.	
1.9.3. Are OV-3 information elements constructed of OV-7 entities?		**2**	**3**		S	As the OV-3 and OV-7 complement each other, there should be two-way traceability and correlation.	
1.10. SV-1: Systems/Services Interface Description (II) [7]							
1.10.1. Is the SV-1 present?	6	6	6	X	C	The SV-1 provides identification of systems nodes, systems, system items, services, and service items and their interconnections, within and between nodes	DoDAF, section 5.1

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
1.10.2. Are SV-1 interfaces implemented by SV-2 communications link(s) or communications network(s)?	6	6	6	6	C	The SV-1's interfaces must be implemented by the SV-2's communications link(s) and/or communication network(s). The SV-2's communications links and/or communications networks details must be consistent with those of the interfacing systems. This will provide consistency in interoperability testing and certification.	
1.10.3. Are SV-4 system functions executed by systems defined in SV-1?	6	6	6	6	C	The SV-4 system functions must be executed by systems defined in the SV-1. This will provide consistency in interoperability testing and certification.	
1.10.4. Do SV-1 systems match SV-5 systems?	6	6	6	X	C	The SV-1 systems must match the SV-5 systems. This will provide consistency in interoperability testing and certification.	
1.11. SV-2: Systems/Services Communications (II) [7]							
1.11.1. Is the SV-2 present?	X	X	X	6	C	The SV-2 describes how physical media support interfaces. The SV-2s are more important now that SV-1s are no longer required. Check and double-check all data.	DoDAF, section 5.2
1.11.2. Can you determine SV-2 interfaces/ interface criticality?(???AHM)	X	X	X	6	C	The SV-2 associates a system node or facility with an operational node. Note: If an SV-1 is not available to depict key interfaces of which one of the criteria of being a key interface is whether the interface is mission critical, then the SV-2 should reflect this detail.	
1.11.3. Does the SV-2 provide system node/facility linkage to an OV-2 operational node and is it correct?	X	X	X	6	C	Bridging of operational and system views depends on the rules used to create the SV-2. DoDAF definition says SV-2 documents the kinds of communications media that support the systems and implements their interfaces as described in SV-1. Thus, SV-2 shows the communications details of SV-1 interfaces that automate aspects of the needlines represented in OV-2.	

X. Requirement X.X Potential Issue(s)	**CDD**[4]	**CPD**[4]	**ISP**[4]	**TISP**[4]	**Maximum Level of Criticality**[5]	**Guidance**	**Reference**[1]
1.11.4. Does the SV-2 provide depiction of data flow details and/or is the data flow properly associated with interface(s)?	X	X	X	6	C	The SV-2 provides detail on paths of data flows. The SV-2 associates data flows with interfaces and interface criticality.	
1.11.5. Do the SV-2 communications link(s) or communications network(s) implement the SV 1 interfaces?	6	6	6	6	C	The SV-1's interfaces must be implemented by communications links or communications networks shown in the SV-2. This will provide consistency in interoperability testing and certification.	
1.11.6. If program/system is a producer and/or consumer of NCES, does the SV-2 identify a service registry?	X	X	X	6	C	The SV-2 needs to reflect the service registry, which is a platform neutral, network, based directory that stores information about services and is searchable based on the descriptive metadata defined in the service specification.	
1.12. SV-4a and 4b: Systems/Services Functionality (II)[7]							
1.12.1. Is the SV-4 present?	X	X	X	6	C	The SV-4 must describe what system function/s implement which system data flows. Additionally, the SV-4, to make an effective bridge to the TV-1, should identify which standards are used to implement a function	DoDAF section 5.4.1 and 5.4.3
1.12.2. Are the SV-4 systems/services functions traceable through the SV-2, system data flow, to the OV-5 operational activities?	X	X	X	6	S	System functions from the SV-4 are implementing the operational activities.	
1.12.3. Are SV-4 system functions executed by systems defined in SV-1?	6	6	6	6	S	The SV-4's system functions must be executed by systems defined by the SV-1. This will provide consistency in interoperability testing and certification.	
1.12.4. Do SV-4 system functions map one-to-one to system functions in SV-5?	X	X	X	6	S	The SV-4's system functions must map one-to-one to the SV-5's system functions. Consistency of mapping supports more accurate interoperability testing and certification. This will provide consistency in interoperability testing and certification.	

X. Requirement X.X Potential Issue(s)	**CDD**[4]	**CPD**[4]	**ISP**[4]	**TISP**[4]	**Maximum Level of Criticality**[5]	**Guidance**	**Reference**[1]
1.12.5. Do SV-4 system data flows map to system data elements appearing in system data exchanges of SV-6?	X	X	X	6	S	The SV-4's system data flows must map to the system data elements that make up the system data exchanges in the SV-6. These include the sending and receiving systems (i.e., show data flow direction), needlines, and organizations/nodes. This will provide consistency in interoperability testing and certification.	
1.12.6. For system functions that are common to the JCSFL, are JCSFL function names and definitions used to the maximum extent possible?	X	X	X	6	S (C)	Use of standard function names and definitions (i.e. per the JCSFL) greatly facilitates interoperability testing and certification. We should review the function names against the JCSFL and comment on any errors. If the error could seriously affect our testing, the comment should be made critical. https://www.us.army.mil/suite/page/419489	Encl E, para 3.b.(1)(j) 1
1.12.7. For system functions that are NOT common to the JCSFL, are domain specific names and definitions shown in the SV-4 and SV-5?	X	X	X	6	S	Use of consistent, system-defined function names and definitions greatly facilitates interoperability testing and certification.	Encl E, para 3.b.(1)(j)1
1.13. SV-5: Operational Activity to Systems Function, Operational Activity to Systems and Services Traceability Matrices (II) [7]							
1.13.1. Is the SV-5 present?	X	X	X	X	C	The SV-5 provides a matrix that cross flows operational activities against system functions to depict relationship between the two.	DoDAF section 5.5.1 and 5.5.3
1.13.2. Do the SV-4 systems/services functions map to SV5 systems/services functions?	X	X	X	6	C	System functions in the SV-5 are derived from the SV-4.	
1.13.3. Do the OV-5 operational activities map to SV-5 operational activities?	X	X	X	X	C	Operational activities in the SV-5 are derived from the OV-5.	
1.13.4. Are the OV-5 Operational activity(s) supported by multiple SV-4 system function(s) complete?	X	X	X	6	C	The SV-5 should depict logical relationships of operational activities to system functions.	

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
1.13.5. Do the SV-5 operational activities match OV-5 operational activities?	X	X	X	X	C	The SV-5's operational activities must match the OV-5's operational activities. This will facilitate more accurate interoperability testing and certification.	
1.13.6. Do the capabilities associated with a specific sequence in OV-6c match an SV-5 capability?	X	X	X	X	C	The capabilities associated with a specific sequence in the OV-6c must match the capabilities in the SV-5. This will facilitate more accurate interoperability testing and certification.	
1.13.7. Do SV-5 systems match the SV-1 systems?	6	6	6	X	C	The SV-5's systems must match the SV-1's systems. This will facilitate more accurate interoperability testing and certification.	
1.13.8. Do SV-5 system functions map one-to-one to system functions in SV-4?	X	X	X	6	C	The SV-5's system functions must map one-to-one to the SV-4's system functions. This will facilitate more accurate interoperability testing and certification.	
1.13.9. For system functions that are common to the JCSFL, are JCSFL function names and definitions used to the maximum extent possible?	X	X	X	X	S(C)	We should review the function names against the JCSFL and comment on any errors. If the error could seriously affect our testing, the comment should be made critical. The following URL takes you to where the JCSFL resides on AKO (must be logged into AKO and paste URL into address line: https://www.us.army.mil/suite/page/419489	Encl E, para 3.b.(1)(j)1
1.13.10. For system functions that are NOT common to the JCSFL, are domain specific names and definitions shown in the SV-4 and SV-5?	X	X	X	6	S	Use of consistent, system-defined function names and definitions may facilitate interoperability testing and certification. When mission threads are institutionalized as one approach to interoperability evaluation, we may well be concerned with consistently named operational activities and functions, some of which may be reflected in system function names.	Encl E, Para 3.b.(1)(j)1
1.14. SV-6: Systems/Services Data Exchange Matrix (I)[7]							
1.14.1. Is the SV-6 present?	X	X	X	X	C	The SV-6 must contain data elements and attributes required to develop testing measures for applying criteria of the NR KPP (related to the integrated architecture element).	DoDAF, section 5.6

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
1.14.2. Are all the system data exchange parameters entered in the SV-6?	X	X	X	X	C	Timeliness, criticality, availability, frequency (or periodicity), throughput, size, etc. must be found within the SV-6. Review the system data exchange attributes to be sure the SV-6 entry captures every attribute you need and that the values entered into the SV-6 matrix are within accepted value ranges, measurable, and testable, e.g. speed of light entry for timeliness attribute is unacceptable.	
1.14.3. Does SV-6 describe, in tabular format, system data exchanged between systems?	X	X	X	X	C	The focus of SV-6 is on how the system data exchange is implemented, in system-specific details covering periodicity, timeliness, throughput, size, information assurance, and security characteristics of the exchange. In addition, the system data elements, their format and media type, accuracy, units of measurement, and system data standard are also described in the matrix. The SV-6 data exchange description format includes an interface identifier, which should certainly map to one of the interfaces identified in the SV-1, or referenced in the SV-2.	
1.14.4. Are standards reflected in the SV-6 depicted against system interfaces and are they from the TV-1/TV-2?	X	X	X	X	C	The SV-6 should have column for Data Standards and the standards should be reflected in the TV-1 as well as in DISRonline.	
1.14.5. Are all the system data exchange parameters in a CDD?	X	X	X	X	S	CDDs may have many TBDs in the SV-6.	

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
1.14.6. Does each SV-6 system data exchange element map to an OV-3 information exchange?	X	X	X	X	C	The OV-3's automated data information elements must map to the system data elements that make up the system data exchanges in the SV-6. These include the sending and receiving systems (i.e., show data flow direction), needlines, and organizations/nodes. This will provide consistency in interoperability testing and certification.	
1.14.7. SV-4 system data flows should map to system data elements appearing in system data exchanges of SV-6.	X	X	X	X	C	The SV-4's system data flows must map to the system data elements that make up the system data exchanges in the SV-6. These include the sending and receiving systems (i.e., show data flow direction), needlines, and organizations/nodes. This will provide consistency in interoperability testing and certification.	
1.14.8. If program/system is a producer and/or consumer of NCES, does the SV-6 identify the Web Services Description Language (WSDL) data?	X	X	X	X	C	WSDL is an XML-based language that provides a model for describing Web services	
1.15. SV-11: Physical Schema (I)[7]							
1.15.1. Is the SV-11 present?		**2**	**3**		C	System data elements defined in the SV-6 should be reused in the SV-11.	DoDAF, section 5.11
1.15.2. Is the physical organization of the data of the SV-11 consistent with the OV-7?		**2**	**3**		S	The SV-11 is the complement to the OV-7.	
1.16. TV-1: Technical Standards Profile (I)[7] https://disronline.disa.mil/a/DISR/index.jsp (log in required)							

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
1.16.1. Is the TV-1 present?	X	X	X	X	C	The TV-1 is only designated non-Critical if a sufficient SV-4 exists. The SV-4 must associate system functions to standards (standards may constrain or enhance the associated system function), otherwise the TV-1 becomes Critical for determining standard conformance implementation. TV-1 must be generated from the DISRonline tool and pasted into the document (CDD, CPD, and ISP) submission. The TV-1 must be posted to SIPRNet DISRonline for compliance.	DoDAF, section 6.1
1.16.2. Does the TV-1 provide applicable standards and/or KIPs/GESPs?	X	X	X	X	C	The standards in the TV-1 should apply to SV-1 systems, subsystems, and system hardware/software; to SV-2 communications systems, communications links, and communications networks; and SV-4 system functions. The TV-1 listed standards may apply to and sometimes constrain data elements in the SV-6.	
1.16.3. Do technical standards in TV-1 apply to modeling techniques in OV-7?		2	3		S	Where TV-1 standards apply to modeling techniques in the OV-7, the traceability should be obvious and should be noted or discussed in the document.	
1.16.4. Do technical standards in TV-1 apply to and sometimes constrain systems, subsystems, and system hardware/software items in SV-1?	X	X	X	X	S	Where TV-1 standards constrain the system or a system component, the constraint must be traceable between the TV-1 and affected hardware/software items in the SV-1. The constraint should also be listed in the AV-1.	
1.16.5. Do technical standards in TV-1 apply to and sometimes constrain communications systems, communications links, and communications networks in SV-2.	X	X	X	X	S	Where TV-1 standards constrain a communications-related component, the constraint must be traceable between the TV-1 and the affected communications item (communications system, link, or network) in the SV-2. The constraint should also be listed in the AV-1.	
1.16.6. Do technical standards in TV-1 apply to and sometimes constrain system data elements in SV-6?	X	X	X	X	S	Where TV-1 standards constrain data elements, the constraint must be traceable between the TV-1 and the affected data element in the SV-6. The constraint should also be listed in the AV-1.	

X. Requirement X.X Potential Issue(s)	**CDD**[4]	**CPD**[4]	**ISP**[4]	**TISP**[4]	**Maximum Level of Criticality**[5]	**Guidance**	**Reference**[1]
1.16.7. Do technical standards in TV-1 apply to modeling techniques in SV-11?	X	X	X	X	S	Where TV-1 standards apply to modeling techniques in the SV-11, the traceability should be obvious and should be noted or discussed in the document.	
1.16.8. Do technical standards in TV-1 reflect, if applicable, NCES standards from DISROnline?	X	X	X	X	S	Where TV-1 standards apply to NCES, the TV-1 should reflect these type standards from DISROnline, i.e., Web Services Description Languages, XML Schema Part 1, XML Schema Part 2, Universal Detection, Discovery and Integration, etc…	
1.17. TV-2: Technical Standards Forecast (III) [7]							
1.17.1. Is the TV-2 present?	X	X	X	X	S	The TV-2 delineates the standards that will potentially affect the relevant system elements (from the SV-1, SV-2, SV-4, SV-6, and OV-7). TV-2 must be generated from the DISRonline tool and pasted into the document (CDD, CPD, and ISP) submission. The TV-2 must be posted to SIPRNet DISRonline for compliance	DoDAF, section 6.2
2. Net-Centric Data and Services Strategy Data: http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf Services: http://www.defenselink.mil/cio-nii/docs/Services_Strategy.pdf							
Note: Tactical systems, control systems, and weapons systems with time critical constraints are exempted from the requirement to demonstrate compliance with the data strategy. However, after-action reporting should follow the data strategy where feasible							Encl E, para 3.b.(2)(b)1
2.1. Is compliance with the DoD Net-centric data strategy documented/referenced?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C	Data strategy compliance details are required for planning and testing, if applicable	Encl E, para 3.b.(2)(b)1

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
2.2. Is compliance with the DoD Net-centric service strategy documented/referenced?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C	Service strategy details are required for planning and testing, if applicable	Encl E, para 3.b.(2)(b)1
2.3. Data and services must be visible.							
2.3.1.Do data assets have associated metadata?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C	Data and service visibility details are required for planning and testing, if applicable	Encl E, para 3.b.(2)(b)4.a.(1)
2.3.1.1. Is the metadata compliant with the DoD Discovery Metadata Specification (DDMS)?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		Encl E, para 3.b.(2)(b)4.a.(1)
2.3.1.2. Are semantic and structural metadata registered in the DoD Metadata Registry (MDR)?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		Encl E, para 3.b.(2)(b)4.a.(1)
2.3.2.Are services registered in the NCES Service Registry?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		Encl E, para 3.b.(2)(b)4.a.(2)

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
2.3.3.Are Web Services Description Languages (WSDL) service descriptions, XML schema definitions (XSD), XML instances, data models, and other appropriate artifacts registered in the MDR?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		Encl E, para 3.b.(2)(b)4.a.(3)
2.3.4.Are Universal Resource Identifiers (URI) for the operational end points registered in the NCES Services Registry?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		Encl E, para 3.b.(2)(b)4.a.(4)
2.4. Data and services must be accessible.							
2.4.1.Are data assets available in shared spaces?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C	Data and service accessibility details are required for planning and testing, if applicable	Encl E, para 3.b.(2)(b)4.b.(1)
2.4.2.Does the program have a written policy on how to gain access to the data, if it is not available to all users?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		Encl E, para 3.b.(2)(b)4.b.(2)
2.5. Data and services must be understandable.							
2.5.1.Are the associated semantic and structural metadata in the Enterprise Catalog?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C	Data and service understandability details are required for planning and testing, if applicable.	Encl E, para 3.b.(2)(b)4.c.(1)

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
2.5.2.Do the keywords entered in the DDMS record in the catalog reflect common user terms, appropriate for mission area or data type, understandable, and conform with MDR requirements that map back to COI identified mission data.	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		Encl E, para 3.b.(2)(b)4.c.(1)
2.5.3.Are metadata associated with the services published in the NCES Service Registry?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		Encl E, para 3.b.(2)(b)4.c.(2)
2.6. Data and services must be secure.							
2.6.1.Do data assets have associated security metadata, and an authoritative source for the data identified?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C	Data and service security details are required for planning and testing, if applicable.	Encl E, para 3.b.(2)(b)4.d.(1)
2.7. Data and services must be interoperable.							
2.7.1.Are semantic, structural and security artifacts for data sharing derived from the Universal Core (Ucore), domain cores (e.g. C2 Core), COIs, or other data standards					S	CJCSI 6212.01E requires the use of "Universal Core (Ucore), domain cores (e.g. C2 Core), COIs, and other data standards". The Defense IEA requires the use of Ucore. https://www.ucore.gov/	Encl E, para 3.b.(2)(b)4.e.(1)
2.8. Exposure Verification Tracking Sheets https://jcpat.disa.mil/JCPAT/AgreeToUsageTerms.do							
Note: Compliance with data and service exposure verification tracking policy is not required for programs with point to point or platform centric information exchanges and does not apply to transmission devices such as radios, satellites, or to network equipment that is otherwise accounted for in the programs architecture views.							Encl E, para 3.b.(2)(b)5

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
2.9. Data Exposure Verification Tracking Sheet							
2.9.1.Slide Title: Is the name of the Program of Record (POR)/System of Record (SOR) being exposed correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C	The data in the data and services exposure verification is required for planning and testing.	Exposure Verification Sheet Guide, version 1.4, para 7.1
2.9.2.PM/phone: Is the name and phone number of the person responsible for management of the POR/SOR correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.3.POC/phone: Is the POC name and phone number of the person who will be responsible for updating and submitting the Exposure Verification Sheets correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.4.Web Page URL: Is the web page Uniform Resource Locator (URL) address of the data being exposed correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.5.IT System, DITPR ID no.: Is the name of the primary system on which the POR/SOR is running correct? Note: The system name is normally registered in the DITPR.	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
2.9.6.Top Level JCA: Is the top-level JCA correct? http://www.dtic.mil/futurejointwarfare/cap_areas.htm	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.7.Data Asset: Is the name of the data asset registered in the Enterprise Catalog?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.8.Description: Is the description of the data being exposed accurate and complete?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.9. Number of objectives: Is the count of the number of achieved areas relative to the previous submission correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.10. Submission date: Is the submission date correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.11. Issues/comments: Do any issues have an impact on planning and testing?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
2.9.12. Exposure start/complete dates: Are the dates of the beginning and end of the exposure effort correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.13. Visibility criteria: Is the content discovery and delivery status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.14. Accessibility criteria: Is the policy status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.15. Accessibility criteria: Is the operational status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.9.16. Understandability criteria: Is the user criteria status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10. Service Exposure Verification Tracking Sheet							

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
2.10.1. Slide Title: Is the name of the Program of Record (POR)/System of Record (SOR) being exposed correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C	The data in the data and services exposure verification is required for planning and testing.	Exposure Verification Sheet Guide, version 1.4, para 7.2
2.10.2. PM/phone: Is the name and phone number of the person responsible for management of the POR/SOR correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.3. POC/phone: Is the POC name and phone number of the person who will be responsible for updating and submitting the Exposure Verification Sheets correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.4. MDR Namespace: Is the registered MDR governance namespace correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.5. IT System, DITPR ID no.: Is the name of the primary system on which the POR/SOR is running correct? Note: The system name is normally registered in the DITPR.	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.6. Top Level JCA: Is the top-level JCA correct? http://www.dtic.mil/futurejointwarfare/cap_areas.htm	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
2.10.7. Service name: Is the service registered in the NCES Services Registry (UDDI) correctly?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.8. Service type: Is the type of service correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.9. MDR Submission: Is the service as it is registered in the NCES Services Registry (UDDI) correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.10. Description: Is the description of the service being exposed accurate and complete?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.11. Number of objectives: Is the count of the number of achieved areas relative to the previous submission correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.12. Submission date: Is the submission date correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
2.10.13. Issues/comments: Do any issues have an impact on planning and testing?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.14. Exposure start/complete dates: Are the dates of the beginning and end of the exposure effort correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.15. Visibility criteria: is the MDR status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.16. Visibility criteria: is the UDDI status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.17. Accessibility criteria: Is the UDDI status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.18. Accessibility criteria: Is the policy status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		

X. Requirement X.X Potential Issue(s)	**CDD**[4]	**CPD**[4]	**ISP**[4]	**TISP**[4]	**Maximum Level of Criticality**[5]	**Guidance**	**Reference**[1]
2.10.19. Understandability criteria: Is the MDR status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
2.10.20. Understandability criteria: Is the COI status correct?	X	X	X	X	CDD - S MS B ISP-S CPD-C MS C ISP-C ISP Annex-C		
3. GIG Technical Guidance							
Note: Until the GTG is officially released, programs are required to continue to use KIPs. Use 3.1 until the GTG is officially released.							
3.1. KIP Declaration table							
3.1.1.Is the KIP declaration table in the correct version and format?	X	X	X	X	C	The latest version and format of the KIP declaration table is available at https://www.us.army.mil/suite/page/477323. You will first need access to AKO/DKO then you will insert the web address in address line. Your comment should direct the program to the web site for the table and up-to-date KIP information.	CJCSI 6212.01D App A to Encl D, para 4
3.1.2.Does the KIP version in the KIP Declaration Table agree with the version in the DISROnline?	X	X	X	X	C	Check the DISRonline for the correct version. https://disronline.disa.mil/a/DISR/index.jsp. Your comment should direct the program to the web site for the correct version and status of the KIPs.	CJCSI 6212.01D App A to Encl D, para 4

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
3.1.3.Is the Applicable column correctly filled in?	X	X	X	X	C	KIPs the system will implement should have a 'Yes' in the appropriate cell. You need to compare the KIPs to the TV-1 to make sure the KIPs are correctly marked as applicable or not applicable.	CJCSI 6212.01D App A to Encl D, para 4
3.1.4.Is the DISR status correct?	X	X	X	X	C	Check the DISRonline for the correct status. The DISR status of a KIP can be mandated, emerging, or retired. https://disronline.disa.mil/a/DISR/index.jsp	CJCSI 6212.01D App A to Encl D, para 4
3.1.5.Is the implementation phase designated for each applicable KIP?	X	X	X	X	C	We have to know if the implementation phase is threshold or objective.	CJCSI 6212.01D App A to Encl D, para 4
3.1.6.Is the program producing or consuming the service/data used by the KIP?	X	X	X	X	C	We have to know if the KIP is acting as a consumer or provider for the system.	CJCSI 6212.01D App A to Encl D, para 4
3.1.7.Does each applicable KIP have implementation issues and/or KIP options correctly filled out?	X	X	X	X	C	Implementation issues and KIP options will have a direct bearing on testing.	CJCSI 6212.01D App A to Encl D, para 4
3.1.8.Are the standards referenced in the KIP included in the TV-1?	X	X	X	X	S	In order to correctly test and report on the system, all standards referenced in the KIP must be included in the TV-1.	CJCSI 6212.01D App B to Encl D, para 5.a.(1)(b)
3.2. Note: After the GTG is officially released, programs are required to use the GTG, including GESPs. Use 3.2 after the GTG is officially released.							Encl E, para 3.b.(1)(g)
3.2.1.Does the document contain a preliminary declaration of the functional implementation features and technical capabilities and identify which GESP technical implementation profiles?	X		X	X	CDD-S MS B ISP-S	The GTG declaration is required for planning and testing.	Encl E, 3.b.(3)(c)1

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
3.3. Does the document contain a final declaration of the functional implementation features and technical capabilities and identify which GESP technical implementation profiles		X	X	X	CPD-S MS C ISP-S	The GTG declaration is required for planning and testing.	Encl E, 3.b.(3)(c)2
3.4. See 1.17 for TV-1 and 1.18 for TV-2.						The TV-1 lists the selected mandated standards, and the TV-2 lists emerging and other standards, waivers for retired standards, and acknowledgment of risk for emerging standards. Together, the TV-1and the TV-2 provides the set of standards governing the system's design and implementation. These standards and their justifications (i.e., waivers and risks) provide the basis for interoperability testing and certification.	
4. IA Compliance							
4.1. Does the CDD describe how the system will implement IA policies and procedures?	X				S	As IA threats are constantly changing and cover a spectrum of vulnerabilities (i.e., from operating systems to applications), a system's IA posture must be up to date and flexible. The CDD must show overall understanding of the spectrum of threats, vulnerabilities, and defense measures (e.g., defense in depth). This approach will facilitate the approach to IA testing and validation.	Encl E, 3.b.(4)(b)1
4.2. If encryption (including Public Key Infrastructure (PKI)) technology is required, include a statement that encryption technology will be acquired as part of this effort and will be installed and used, including initial fielding efforts, to ensure information security over all voice, video, and data transmission.	X				S	As encryption is a fundamental IA strategy, it is vital to properly install, use, maintain, and update equipment, software, and keys. Users and administrators must be trained in proper use to prevent compromise. This approach will facilitate IA testing and validation.	Encl E, 3.b.(4)(b)1

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
4.3. Does the document provide the contact information for all the information assurance documentation described in Enclosure D along with an IA compliance statement?	X				A	IA Compliance statement example: "This program or system will be in full compliance with the IA requirements in DOD 8500 series and CJCS 6510 series directives, instructions and manuals."	Encl E, 3.b.(4)(b)2
4.4. Does the CPD describe, in greater detail than the CDD, how the system will implement IA policies and procedures?		X			S	As IA threats are constantly changing and cover a spectrum of vulnerabilities (i.e., from operating systems to applications), a system's IA posture must be able to quickly and specifically adapt to newly cognized threats. The CPD must show detailed understanding of types of threats, vulnerabilities, and defense measures (e.g., how firewalls perform at different levels). This approach will facilitate detailed IA testing and validation.	Encl E, 3.b.(4)(c)1
4.5. If encryption (including Public Key Infrastructure (PKI)) technology is required, include a statement that encryption technology will be acquired as part of this effort and will be installed and used, including initial fielding efforts, to ensure information security over all voice, video, and data transmission.		X			A	As encryption is a fundamental IA strategy, it is vital to properly install, use, maintain, and update equipment, software, and keys. Users and administrators must be trained in proper use to prevent compromise. This approach will facilitate IA testing and validation.	Encl E, 3.b.(4)(c)1
4.6. Does the CPD provide an IA compliance statement?		X			A	IA Compliance statement example: "This program or system is in full compliance with the IA requirements in DOD 8500 series and CJCS 6510 series directives, instructions and manuals."	Encl E, 3.b.(4)(c)2
4.7. Does the CPD provide the contact information for all the information assurance documentation described in Enclosure D?		X			S	The human factor is vital in a system's IA posture. Liaison with the system's IA personnel increases assurance that the IA posture is correctly installed, maintained, updated, and altered (when necessary) in a timely manner. This approach will facilitate IA testing and validation.	Encl E, 3.b.(4)(c)2
5. Supportability							

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
5.1. Spectrum Certification							
5.1.1.Is the spectrum certification status documented (DD Form 1494)? DD1494: http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd1494.htm	X	X			S	Advance spectrum certification helps identify communications capabilities and constraints (e.g., available frequencies, robustness of networks). This will allow additional interoperability tests that will replicate such potential conditions.	Encl E, 3.b.(5)(a)3
5.1.2.Has permission been obtained from designated authorities of sovereign ("host") nations (including the United States) to use that equipment within their respective borders (DD Form 1494)?	X	X			S	Advance HNA increases assurance that the system will successfully communicate within the proposed deployment area. Communications constraints (e.g., limited power grid, interference) will be identified in advance. This will allow additional interoperability tests that replicate such potential conditions.	Encl E, 3.b.(5)(a)7

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
5.1.3.Does the document contain a spectrum compliance statement?	X	X	X	X	S	Sample statement: "Spectrum Supportability. Procurement or acquisition of this wireless, spectrum dependent device will be conducted IAW DOD guidance (e.g., DODD 3222.3, DODD 4650.1, DODI 4630.8, DODD 5000.1, and DODI 5000.2) as well as applicable Military Department (MILDEP) publications. An application for equipment frequency allocation (i.e., DD Form 1494) was (will be) initiated on (date). The DD Form 1494, Application for Equipment Frequency Allocation, was (will be) releasable for coordination purposes to those foreign countries (host nations) in which permanent deployment or lengthy temporary use is contemplated. The program manager (PM) acknowledges that, before assuming contractual obligations for deployment, testing, production, or procurement of this spectrum dependent system, the required spectrum support is or will be available in those host nations determined by the PM or procurer for the equipments intended use. The PM has (will develop) a plan to obtain appropriate equipment allocation guidance/status prior to MS B or MS C as outlined in DODD 4650.1 in order to progress to the next phase."	Encl E, 3.b.(5)(a)11
5.2. Tactical Data Link Implementation							
5.2.1.Are platform TDL implementation details identified?	X	X	X	X	C	**Note:** Identification of each TDL protocol and its details will provide understanding of throughput; performance, timeliness, and multi-unit transmit/receive requirements. This will provide better understanding for performance testing.	Encl E, 3.b.(5)(d)
5.3. Bandwidth Analysis							

X. Requirement X.X Potential Issue(s)	**CDD[4]**	**CPD[4]**	**ISP[4]**	**TISP[4]**	**Maximum Level of Criticality[5]**	**Guidance**	**Reference[1]**
5.3.1.Does the Milestone C submission address Bandwidth requirements?		X	X	X	S	Identification of system bandwidth requirements by transmission category and by information sharing category (application, input/output, data type, and transaction type) will result in better understanding of impact upon the GIG. This will result in better end-to-end performance testing.	Encl E, 3.b.(5)(e)
6. Other							
6.1. Are the critical (threshold) and all (critical plus non-critical - objective) requirements, including net-centric requirements, clearly delineated by criticality and increment?	X	X	X	X	C (CPD, MS-C ISP, TISP) S (CDD, MS B ISP)	If the criticality and/or increment of a requirement, net-centric or otherwise, is not clear in a capabilities document, ISP, or TISP; we have to assume it is critical and being implemented in the current increment.	Encl F, para 10.a.(2)
6.2. Does the TV-1 contain non-DISR standards, vendor documentation, or proprietary specification?	X	X	X	X	S	The TV-1 may contain non-DISR standards, specifications, etc. We should provide a Substantive comment to the program if they are included. However, if the non-DISR remain in the J-6 certified TV-1, we will test them to the best of our ability.	
6.3. Is there is any reference to connecting to DSN?	X	X	X	X	C	If the system will connect to the DSN, the Unified Capabilities Requirements (UCR) must be considered. See http://jitc.fhu.disa.mil/tssi/ for additional information.	DODI 8100.3, para 6.1.3.3
6.4. Is there any reference to connecting to the DRSN?	X	X	X	X	C	If the system will connect to the DRSN, the UCR must be included as additional requirements. See http://jitc.fhu.disa.mil/tssi/ for additional information. The user must request connectivity approval from the DRSN PM. If this is not discussed, we should comment as a courtesy to the program.	

JITC Document Review Checklist
CJCSI 6212.01E
Version 1.0, 12 May 2009

X. Requirement X.X Potential Issue(s)	**CDD**[4]	**CPD**[4]	**ISP**[4]	**TISP**[4]	**Maximum Level of Criticality**[5]	**Guidance**	**Reference**[1]
6.5. Is there any reference to the system containing a UHF DAMA SATCOM capability?	X	X	X	X	C	If the system has a UHF DAMA SATCOM capability, CJCSI 6251.01B requirements must be considered. See http://jitc.fhu.disa.mil/reg/uhfdama.html for additional information.	CJCSI 6251.01B
6.6. Does any other KPP address or affect interoperability in any way and are the requirements in the KPP measurable and testable?	X	X	X	X	C	Ensure that all KPPs that may affect interoperability are measurable, testable, and complete.	Encl F, para 1
6.7. Is there enough information provided for you to be able to plan, execute, and report on a Joint Interoperability test?	X	X	X	X	C	You, or someone else at JITC, will have to test the system based on this document. If it is not adequate in any way, you need to make the appropriate comment(s).	Encl F, para 10
6.8. Does the document clearly delineate the requirements between each increment (phase, spiral, block, etc.)?	X	X	X	X	C	If the requirements for each increment cannot be determined, the JITC will have to test and certify to all requirements in the document.	Encl F, para 10.a.(2)
6.9. Is the Acquisition Category (ACAT) included?	X	X	X	X	S	The ACAT helps identify level of effort.	CJCSM 3170.01C, App A to Encl F
6.10. Does the document include a statement on how the program will comply with CJCSI 6130.01, which directs specific measures to protect GPS?	X	X	X	X	S	The statement should either address implementing a SAASM compliant receiver, or obtaing a waiver from ASD(NII).	Encl D, 3.e.(6)(e)

1. All references are to CJCSI 6212.01E, Table E-1, and DoDAF Ver 1.5, Vol. II, unless otherwise noted.
2. Required only when IT/NSS collects, processes, or uses any shared data or when IT/NSS exposes, consumes, or implements shared services.
3. Only required for Milestone C, if applicable (see Note 2).
4. An X in the document column indicates the requirement is applicable to that type of document.
5. Maximum Level of Criticality indicates the maximum level (severity) of comment JITC should submit for this issue.
    a. C: Critical comments are for missing or incorrect information can prevent the JITC from testing and certifying the system.
    b. S: Substantive comments are for missing or incorrect information that may affect the JITC from effectively testing and certifying the system.
    c. A: Administrative comments are for minor errors that do not affect the JITC.

6. Not a mandated action but if reviewer can not determine if data/information is accurate for testing purposes from the architecture product provided recommend contacting PMO to obtain the associated architecture product with regard to this question.
7. All architecture products are required by CJCSI 6212.01E, depending on document type and system functions. The criticality of architecture products, from JITC's perspective, is in the parentheses next to the architecture product name. The levels of criticality are:
    a. I: Critical, these products are required for interoperability testing.
    b. II: Acute, these products can be required for interoperability testing. However, if the critical products are available and correct, the need for these products may be reduced.
    c. III Useful information, these products provide useful information for interoperability testing, but are not required.

Sample comment

Criticality (C, S, A)	**Page #**	**Paragraph #**	**Line #**	**Classification (U, C, S, F)**
C				U
Reviewer:	Jane Doe			
Reviewer Org:	JITC			
Reviewer Email:	jane.doe@disa.mil			
Reviewer Phone:	520-538-1111 or DSN 879-1111			
Comment:	SV-4 lists system functions but does not show data flows. The SV-4 should develop a clear description of the necessary data flows that are input (consumed) by and out put (produced) by each system.			
Recommendation:	Add more detail to show data flows between system functions/systems.			
Rationale:	Clarify data flows/exchanges.			