Net-Ready Key Performance Parameter (NR-KPP) Implementation Guidebook

Version 2.0
30 SEP 2011

Deputy Assistant Secretary of the Navy
(Research, Development, Test, and Evaluation)
Chief Systems Engineer
Department of the Navy
Washington, D.C. 20376

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 SEP 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Net-Ready Key Performance Parameter (NR-KPP) Implementation Guidebook	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Deputy Assistant Secretary of the Navy,, (Research, Development, Test, and Evaluation) ,Chief Systems Engineer,Washington,DC,20376**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

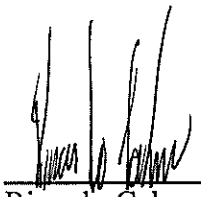
13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**44**	

Approval Page



30 SEPT 2011

Ricardo Cabrera (acting)
Deputy Assistant Secretary of the Navy
(Research, Development, Test & Evaluation)
Chief Systems Engineer

Date

Table of Contents

List of Figures

List of Tables

List of References

(a) Joint Chiefs of Staff Instruction (CJCSI) 3170.01G
(b) DoD Directive 4630.05
(c) DoD Instruction 4630.08
(d) Joint Chiefs of Staff Instruction (CJCSI) 6212.01
(e) DoD Architecture Framework (DoDAF)
(f) DoD Instruction 5000.2
(g) Navy Systems Engineering Resource Center (NSERC) online
(h) OPNAV Instruction 3000.12A, Operational Availability
(i) Universal Joint Task List, JEL, DTIC
(j) OPNAVINST 3500.38B, Universal Navy Task List
(k) Joint Common Systems Function List
(l) The DoD Architecture Registry System (DARS)
(m) Naval Architecture Repository System (NARS)
(n) DoN Enterprise Architecture Repository
(o) Navy Training Information Management System (NTIMS)
(p) Defense Readiness Reporting System (DRRS)
(q) CJCSG 3501, The Joint Training Systems Primer, and the JMETL Development Handbook
(r) OPNAVINST C3501.2, Operation Missions
(s) CES Metadata Registry homepage
(t) (Navy) Common Information Exchange List (CIEL)
(u) National Information Exchange Model (NIEM)
(v) The JITC resource page, NR-KPP Testing Guidebook
(w) Selective Availability Anti-Spoofing Module (SAASM)
(x) Spectrum, and Joint Tactical Radio System (JTRS) requirements
(y) IEEE 1220
(z) Global Information Grid Technical Guidance (GTG) wiki
(aa) Global information Grid Technical Profile (GTP) wiki
(bb) DoD Metadata Registry (MDR)
(cc) Net-Centric Enterprise Services (NCES) Service Registry
(dd) DoD Information Technology Standards Registry (DISR)
(ee) The Defense Acquisition Guidebook (DAG)

1 Executive Summary

This guidebook provides acquisition program sponsors, program managers, and delegated technical support staff with supplementary information for establishing a meaningful, measurable and testable Net-Ready Key Performance Parameter (NR-KPP) for their respective acquisition programs. *The NR-KPP is an operational requirement* representing critical measures of performance for information exchanges directly supporting the intended mission capabilities of DoD-owned/operated systems. The NR-KPP is considered mandatory for all Information Technology (IT) and National Security Systems (NSS) that exchange information across their own system boundary.

Key Performance Parameters are established as critical requirements for military systems by the Joint Capabilities Integration and Development System (JCIDS) as defined by the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G (reference a). Authority for the Net-Ready KPP is established via DoD Directive 4630.05 (reference b) and DoD Instruction 4630.08 (reference c).

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E (reference d) articulates the NR-KPP in terms of a Compliance Statement to be included and addressed in the program's JCIDS documentation, commonly referred to as the Capability Development Document (CDD) and Capability Production Document (CPD), as well as the Information Support Plan (ISP). This guidebook is intended to address the difficulty many programs have had in developing measurable/testable performance parameters from the NR-KPP Compliance Statement. The approach comprises a "Four-Step Process" as follows.

Step One, *Mission Level Systems Engineering Analysis*, involves confirmation/validation (and refinement) of the mission activities that the system will support, and performance measures associated with those activities. **Step Two, *Information Analysis***, sets down the information exchanges necessary to support those mission activities and the information exchange performance parameters (inclusive of the five areas of Information Assurance) necessary to meet the established mission performance parameters. **Step Three, *Systems Engineering / Requirements Derivation***, develops the information needs and performance parameters into system performance requirements and specifications. **Step Four, *NR-KPP Documentation***, takes the results of the previous steps, consolidates and prepares the information specifying the NR-KPP into required formats, and incorporates the completed NR-KPP into the requisite documentation (e.g., the CDD/CPD and ISP).

The supporting documentation includes DoD Architecture Framework (DoDAF) artifacts captured in a DoDAF Meta-Model (DM2) compliant modeling database (see reference e). The importance of the modeling database cannot be stressed enough as it provides the capability to address System-of-Systems and Family-of-Systems interoperability issues in the early phases of development, rather than as "fixes" to problems encountered during testing and deployment.

The approach presented in this guidebook is only one methodology for establishing a program's NR-KPP. The four "steps" of this process are not a prescribed sequential ordering, but a logical grouping of activities for the purposes of systematically addressing the NR-KPP.

2 Introduction

2.1 Background Information

The Net-Ready Key Performance Parameter (NR-KPP) is an operational requirement that represents critical measures of performance for information exchanges directly associated with the ability of a DoD-owned/operated system to provide its intended mission capabilities. It is considered mandatory for all Information Technology (IT) and National Security Systems (NSS) that exchange information across their own system boundary. The Net-Ready Key Performance Parameter was initially established as the Interoperability Key Performance Parameter as part of DoD Instruction 5000.2 of April 2002 (reference f); subsequent revisions of the document have not deleted the operational requirement for interoperability. The Interoperability KPP requirement was later renamed the Net-Ready KPP by the 2004 revisions of DoD Directive 4630.05 (reference b) and the corresponding DoD Instruction 4630.08 (reference c) to emphasize the criticality of effective information exchange via net-centric operations.

Key Performance Parameters (KPPs) are established by the Joint Capabilities Integration and Development System (JCIDS) as defined by the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G (reference a). Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E (reference d) articulates the Net-Ready KPP in terms of a Compliance Statement to be included and addressed in the program's JCIDS documentation, commonly referred to as the Capability Development Document (CDD) and Capability Production Document (CPD), as well as the Information Support Plan (ISP). As with other KPPs, the operational requirements comprising the NR-KPP should result from analyses done as part of the JCIDS process[1].

2.2 Compliance Statement Issues

Acquisition Programs have had some difficulty expressing the Net-Ready KPP in measurable and testable terms, in part because of the way the compliance statement is structured. Its focus is on a set of process constraints instead of measurable and testable performance attributes. As a result, many programs don't understand the intent of the NR-KPP. The temptation is to address the NR-KPP differently than their other Key Performance Parameters (KPPs) and simply ensure they have satisfied the Interoperability & Supportability Certification checklists. The associated artifacts are then minimally relevant to system design, verification, and validation. Ultimately, the lack of clear, concise, measurable and testable performance parameters associated with the NR-KPP can result in fielding Navy systems that are not appropriately net-ready and do not provide the full net-centric capabilities needed.

In March 2007, the Deputy Assistant Secretary of the Navy (DASN) Command, Control, Communications, Computers, Intelligence, and Space (C4I and Space) requested that the ASN (RD&A) Chief Systems Engineer (CHSENG) conduct a Lean/Six Sigma (LSS) project to "find potential process improvements for NR-KPP development, review, and use."[2] In this request,

[1] *Manual for the Operation of the Joint Capabilities Integration and Development System,* https://www.intelink.gov/wiki/JCIDS_Manual.

[2] DASN (C4I and SPACE) memorandum, 30 March 2007, "Review of Net Ready Key Performance Parameter (NR-KPP Impact on Acquisition Programs"

DASN (C4I and Space) expressed interest in identifying ways to adjust the NR-KPP process and documentation to better serve acquisition programs."[3] This project found that:

- The Joint Staff NR-KPP Instruction lacks clarity.
- Operational requirements documents do not specify measurable and testable NR-KPP requirements.
- Programs cannot adequately demonstrate they engineered interoperability into their system.
- The Operational Test and Evaluation (OT&E) community often finds a program's NR-KPP lacks traceability to other requirements.

2.3 Guidebook Approach for addressing the NR-KPP

In response to these challenges, ASN (RD&A) CHSENG developed the NR-KPP Guidebook. The guidebook has been piloted by a small number of acquisition programs, and lessons learned / comments from those programs have been incorporated into this revised version of the guidebook. Readers should keep in mind that the approach described in this guidebook represents one methodology for establishing a program's NR-KPP, and should assess the efficiency and applicability of this process against their own unique programmatic needs.

This Guidebook clarifies the definitions of net-readiness and the NR-KPP. By breaking the development of the NR-KPP into a four-step process, it allows the reader to identify measurable and testable parameters to support an acquisition program's Net-Readiness. The Guidebook then provides a NR-KPP template that parallels the form of the Compliance Statement that programs can use to express their program specific Net-Ready attributes and performance parameters.

The Guidebook is not intended to prescribe redundant steps to the overarching acquisition process; rather it *is* intended to show how the existing mission systems engineering processes are used to produce a traceable, measurable, and testable Net Readiness requirements suitable for use as a Key Performance Parameter. The Guidebook also lists key points that will help ensure the program meets the intent of the NR-KPP. The Guidebook follows the form of its original inception as a "four-step process," described as follows. The four "steps" of this process are not a prescribed sequential ordering of literal procedural steps, but a logical grouping of activities for the purposes of systematically addressing the NR-KPP. Other resources have described the NR-KPP development process in similar terms, with more or fewer "steps," or supporting activities such as the development of supporting documentation arranged differently. The piloting projects for this process indicate that programs may easily follow the four steps as described, or individually pursue each "Information Exchange" thread to completion, or any combination thereof that best fits their program circumstances. What is crucial is that all of the activities contained within the "four step process" are adequately addressed.

The initial step, named ***Mission Level Systems Engineering Analysis***, involves confirmation/validation (and possibly refinement) of the mission activities that the system is intended to support, and the mission performance measures, generally expressed in terms of Measures of Performance/Measures of Effectiveness (MOP/MOE), that are associated with those

[3] Ibid

activities. The full mission analyses are normally done prior to developing any system KPPs. However, in the event the mission analysis was not complete, or if mission parameters have changed, this NR-KPP development process allows for the validation and any necessary updates to that existing analysis. At this writing, a Mission Thread Development Guidebook is under development to assist in the details of this process. It will be published to the Navy Systems Engineering Resource Center (NSERC) online repository as soon as it becomes available.[4] (See reference g.)

The second step, named ***Information Analysis***, involves establishing the information exchanges necessary to support those mission activities and the information exchange performance parameters (inclusive of the five areas of Information Assurance) necessary to meet the established mission performance parameters.

The third step, named ***Systems Engineering / Requirements Derivation***, involves derivation of the information needs and performance parameters into system performance requirements and specifications.

The fourth step of the guidebook process, ***NR-KPP Documentation***, consolidates documentation from the first three steps, prepares the information specifying the NR-KPP into required formats, and incorporates the completed NR-KPP into the Acquisition Documentation that it is intended to support (e.g., the JCIDS capability documents and the Information Support Plan).

Supporting documentation for each of the first three steps will generally include several DoD Architecture Framework (DoDAF) artifacts. The importance of these supporting artifacts is not in the documents or graphics themselves but in the information they communicate, and that that information is either reported from or can be easily captured to a modeling database that is compliant with the DoDAF Meta-Model (DM2). (See reference e.) The importance of the modeling database cannot be stressed enough as it provides the capability to find and address interoperability issues in the early phases of development, rather than as "fixes" to problems encountered in testing and deployment. Information captured in the modeling database will be referenced by the JCIDS documentation for each individual program. The intent is that it can also be re-used throughout the JCIDS process for determining future needs to address emerging missions and associated military capabilities.

[4] Naval Systems Engineering Resource Center (SharePoint site) https://nserc.navy.mil/Pages/default.aspx.

3 Analysis and Clarification of the NR-KPP Compliance Statement

This section clarifies the definitions of net-readiness and the NR-KPP. This clarification is intended to help programs understand the purpose of the NR-KPP so their system can satisfy this important KPP.

3.1 Net-Readiness and its Relationship to Mission Effectiveness

Net-readiness has been defined as the ability to provide and receive mission critical information in a timely manner. Its primary focus is on the performance of system to system information exchanges and it is complemented by the basic tenets of Information Assurance, i.e., availability, integrity, confidentiality, authentication and non-repudiation. The use of networked communications paths is implied, however, most all information handling systems that communicate externally can be described as "networked", even if the network has only two nodes. For information handling systems, a Net-Readiness metric can be described as a Measure of Effectiveness / Measure of Performance that traces back to Mission Effectiveness.

Mission Effectiveness is a Figure of Merit (FOM), or metric, typically used to assess a Warfighting Mission. It is defined simply as the aggregate probability of successfully completing the mission. A component metric, called ***System Effectiveness***, is generally recognized as the probability that the material systems or "tools" used to conduct the mission are ready, and will successfully perform all the necessary system functions once the mission is initiated. Although used somewhat interchangeably, "Measures of Effectiveness" (MOEs) generally indicate how well the operational tasks are accomplished by an organization, and "Measures of Performance" (MOPs) generally indicate how well a system performs a component operational function. A more restrictive but less commonly used definition of MOEs and MOPs delineates MOEs as dimensionless probabilities of success, and MOPs as directly measurable aspects of system performance (dimensioned performance parameters). MOEs/MOPs are mathematically related to overall Mission Effectiveness. The relationship may be modeled in various ways, but the underlying principle is that in order to achieve a desired probability of mission success under specific conditional constraints, a task or activity must be executed to some threshold level of effectiveness or performance under those same constraints.[5] (See reference h.)

Missions are composed of operational tasks; these tasks are often arranged in parallel/sequential maps known as Mission Threads which are used to describe the complete mission. A standardized taxonomy of mission tasks has been developed which includes attributes recommended as MOEs/MOPs, along with mission conditions (conditional constraints) that can affect the tasking. Publication of these mission oriented task lists can be found in the Universal Joint Task List[6] (reference i) and service unique publications such as the Universal Naval Task

[5] Mathematically related definitions of Mission Effectiveness, System Effectiveness, and contributing effectiveness and performance factors are primarily taken from OPNAV Instruction 3000.12A on Operational Availability. Several different resources are available on defining MOEs/MOPs, but that instruction appears to provide the most straightforward illustration for the purposes of this discussion.

[6] An archive of the most recent UJTL is currently maintained within the Joint Electronic Library, hosted by Defense Technical Information Center. http://www.dtic.mil/doctrine/training/ujtl_tasks.htm.

List (OPNAVINST 3500.38B)[7]. (See reference j.) Likewise a standardized taxonomy of system functionality has been developed and published under the Joint Common Systems Function List[8] (reference k). The common systems function list is organized to work with the task list taxonomies, indicating system functions necessary for the performing organization to successfully complete its tasking.

The NR-KPP is intended to capture the information exchange related MOEs/MOPs that support the overarching task metrics. In effect, a net-ready system meets the requirements for both the technical exchange of information and the operational effectiveness of those exchanges[9]. The JCIDS process requires that certain programs satisfy an NR-KPP to ensure those programs field a net-ready, interoperable system. In light of this intent, programs should continually evaluate whether or not their NR-KPP efforts contribute to the development of a net-ready system, and how those net-ready aspects ensure the Mission Effectiveness of the forces employing that system.

3.2 Net-Ready KPP Definition and Verbiage of the Compliance Statement

CJCSI 6212.01E (reference d) defines the NR-KPP as a key parameter stating a system's operational requirements for information, the timeliness of that information, Information Assurance (IA), and net-ready attributes for both the technical exchange of information and the operational effectiveness of that exchange. The instruction articulates this definition in terms of an NR-KPP Compliance Statement as described below. To satisfy the NR-KPP, programs must show that they completely satisfy the capability's information needs in a timely and accurate manner. The Four-Step process described in this guidebook helps programs do this by building on the process described on page E-21 of CJCSI 6212.01E.

The following information is taken directly from CJCSI 6212.01E, enclosure E, Table E2, [The] NR-KPP Compliance Statement. It provides the basis for the NR-KPP in the form of a verbatim compliance statement. The only differences in verbiage between the *compliance measures* used in the "Objective (O)" and "Threshold (T)" columns of the table are in the use of abbreviations. The actual differences in objective and threshold values are the support of "all operational activities identified …" (O), versus the more limited "all *joint critical* operational activities identified…" (T).

3.2.1 NR-KPP Description

Net-Ready: The capability, system, and/or service must *support Net- Centric military operations*. The capability, system, and/or service must be able to *enter and be managed in the network*, and *exchange data* in a secure manner to enhance mission effectiveness. The capability, system,

[7] Department of Navy Issuances can be found, by document number, in the following DONI repository, hosted by the Defense Logistics Agency http://doni.daps.dla.mil/default.aspx.

[8] Information on The Joint Common Systems Function List is currently available at the following portal, under the auspices of USJFCOM J89, Standards and Policy branch: https://www.us.army.mil/suite/page/419489/. The portal is part of the Defense Knowledge Online (DKO) resource portal and requires a login account. At this writing, the Joint Common Systems Function List includes neither recommended MOEs/MOPs nor conditions. "Mission conditions" would presumably flow down from the task list, but it remains the responsibility of the systems engineering team to establish the appropriate MOEs/MOPs as part of the system requirements.

[9] The definition above summarizes the full definition of a net-ready system as stated on page GL-20 of CJCSI 6212.01E.

and/or service must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability.

3.2.2 Objective and Threshold Levels

Threshold: The capability, system, and/or service must fully *support execution of **joint critical** operational activities and information exchanges* identified in the DoD Enterprise Architecture and solution architectures based on integrated DoDAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: [see Compliance Measures]

Objective: The capability, system, and/or service must fully *support execution of **all** operational activities and information exchanges* identified in DoD Enterprise Architecture and solution architectures based on integrated DoDAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: [see Compliance Measures]

3.2.3 Compliance Measures

1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DoDAF content, including specified operationally effective information exchanges
2) Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-Internet Protocol (IP) communications
3) Compliant with Global Information Grid (GIG) Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Technical Profiles (GTPs)[10], formerly known as GIG Enterprise Service Profiles (GESPs), necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views
4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization To Operate (ATO) by the Designated Accrediting Authority (DAA), and
5) Supportability requirements to include Selective Availability Anti-Spoofing Module (SAASM), Spectrum, and Joint Tactical Radio System (JTRS) requirements.

3.3 Analysis of the Net-Ready KPP Compliance Statement

The following sections discuss each area of the NR-KPP Compliance Statement and suggest derived requirements that will help programs understand how to ensure they produce a net-ready system.

[10] CJCSI 6212.01E cites GIG Enterprise Service Profiles (GESPs) as one of the NR-KPP compliance measures. However, within the GIG Technical Guidance Federation, these have been renamed GIG Technical Profiles (GTPs), available at https://www.intelink.gov/wiki/Portal:GIG_Technical_Guidance.

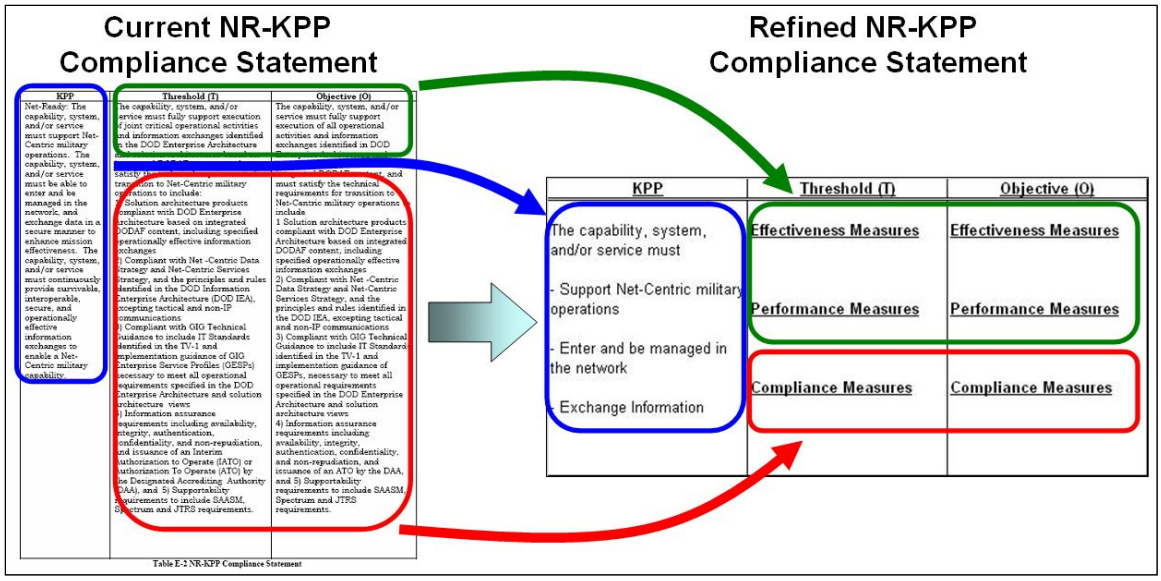


Figure 3-1 Three Components of NR-KPP Compliance Statement

3.3.1 Illustration of the NR-KPP Compliance Statement

Figure 3-1 uses colored boxes to highlight the three areas in the original NR-KPP Compliance Statement. Application of the Four-Step Process will assist in deriving appropriate sub-requirements and measures of effectiveness/performance in the refined NR-KPP Compliance Statement. CJCSI 6212.01E mandates that all programs with an NR-KPP include the NR-KPP Compliance Statement in their Capability Development Document (CDD), Capability Production Document (CPD), and Information Support Plan (ISP), and for Services/Application Joint Staff Interoperability and Supportability (I&S) Certification.

If Resource Sponsors include the NR-KPP Compliance Statement in a program's JCIDS documents, programs must ensure that they satisfy the NR-KPP Description as measured by the NR-KPP Effectiveness and Performance Measures and NR-KPP Compliance Measures. Because programs typically focus on the NR-KPP Compliance Measures and ignore the NR-KPP Effectiveness and Performance Measures, programs may or may not satisfy all elements of the NR-KPP Description. Furthermore, in order to successfully complete Milestone and Gate Reviews, programs must be able to articulate how their system satisfies the NR-KPP Description in terms of the NR-KPP Effectiveness and Performance Measures as well as the NR-KPP Compliance Measures. The Four-Step Process proposed in this guidebook will help programs do these things by providing a mechanism for satisfying all three NR-KPP components.

3.3.2 Net-Ready KPP Description

The NR-KPP description contains the attributes used to determine whether a system is net-ready. As stated in the NR-KPP description, a net-ready system must have three attributes. The system must: 1) support net-centric military operations, 2) enter and be managed in the network, 3) exchange information in a continuously survivable, interoperable, secure, and operationally effective manner, to enable Net-Centric military capability.

3.3.2.1 Attribute 1: Support Net-Centric Military Operations

This attribute consists of specifying which military operations (e.g., missions or mission threads) a system supports, under what conditions they can be supported, and the effectiveness metrics for

evaluating mission success. The list should be further decomposed to specify the operational (and tactical) tasks needed for the system to support those military operations (missions). The conditions under which the tasks are performed should remain the same as for the mission. Note that for the purposes of the final NR-KPP documentation this attribute need only include net-ready tasks. In this case, a task is defined as net-ready if it produces information for an external system (including storing data on an external system) or consumes information from an external system.

It is likely that the systems overarching mission thread will have already been documented by the operational sponsor. It is the further decomposition to elemental, operator level tasking, and identification/elicitation of the specifically Net-Ready tasks that will require additional effort from the program's technical authority and systems engineering team.

The Joint Mission Essential Task List (JMETL) framework, and service specific Mission Essential Task Lists, provide standardized mechanisms for specifying this element. These Mission Essential Task Lists, conditions, and recommended effectiveness metrics are described in the Universal Joint Task List (UJTL)[11], (see reference i). For Navy and Marine Corps specific tasking, see OPNAVINST 3500.38B – the Universal Naval Task List (UNTL)[12], (see reference k). Although the training community created the UJTL and UNTL to describe training requirements for current operations, their framework and content provide a convenient and effective framework for developing derived requirements (Effectiveness and Operational Performance Measures). Refer to the Naval Warfare Plan[13] specific to the mission in question in order to properly sequence the tasks along a timeline. If operation of the system/platform is limited to certain geographical areas, refer to Navy Tactics, Techniques, and Procedures for additional guidance.

3.3.2.2 Attribute 2: Enter and Be Managed In the Network

This attribute specifies which networks and external systems the system must connect to in order to exchange the information necessary to support the previously listed Operational Tasking. The phrase "enter and be managed in the network" implies many of the attributes that are part of the Information Assurance domain, such as authentication and non-repudiation. At this point, this net-ready attribute does not have a standardized framework of terminology and metrics like the Universal Joint Task List (UJTL). Programs may take the approach of asking a series of questions to develop the derived requirements of this attribute. These questions should be in the context of the missions and tasks that the program supports, and include:

- What types of networks will the system connect to? The response is not limited to Internet Protocol (IP) networks; may include radio networks or military specialized communications networks.

[11] An archive of the most recent UJTL is currently maintained within the Joint Electronic Library, hosted by Defense Technical Information Center http://www.dtic.mil/doctrine/training/ujtl_tasks.htm

[12] Department of Navy Issuances can be found, by document number, in the following DON repository, hosted by the Defense Logistics Agency http://doni.daps.dla.mil/default.aspx

[13] Naval Warfare Plans are maintained by the Naval Warfare Development Command (NWDC), in a classified repository. Contact NWDC for further information, https://www.nwdc.navy.mil/default.aspx

- What metrics do the required networks use to measure network entrance and management performance? This should include metrics used to measure the time from system start up to when the system has connected to the network and is supporting military operations.
- Who will manage the system as it connects to various networks?
- How will the system be managed? Will management be distributed, centralized, local, remote, etc.?
- What configuration parameters does the network have?

3.3.2.3 Attribute 3: Effective Information Exchanges

This attribute specifies the Information Elements produced and consumed by each mission and task identified in with regard to Support of Net-Centric Military Operations. The focus is on external system interactions, therefore the attribute need only identify 1) Information Elements produced, sent, or makes available to an external system; 2) Information Elements received from an external system. For each Information Element, the attribute should specify operational performance metrics used to measure the effectiveness of the Information Element's production or consumption. As stated in the NR-KPP Description, the performance metrics should describe the elements' continuous survivability, interoperability, security, and operational effectiveness. Programs should consider how these metrics may affect "unanticipated users"[14] of the Information Elements, e.g. if future systems can readily be made "back-compatible" with the information exchange media, format, content, etc.

The DoDAF OV-3 Operational Information Exchange Matrix and SV-6 System Data Exchange Matrix provide sample operational performance metrics for the information production and consumption. Under DoDAF v2.0, the OV-3 is called the Operational Resource Flow Matrix, but still provides the performance metrics, and can be used for information flows. In DoDAF v2.0, the SV-6 is called the System Resource Flow Matrix.

Table 1 below summarizes the NR-KPP Attributes in terms of:

- Refined attributes and their associated metrics
- Standardized frameworks and data sources to leverage when specifying the attributes
- Component of the NR-KPP using the attribute

[14] Unanticipated users are those with legitimate/authorized need for the data, but do not provide advance notification that they will use it.

Table 3-1: NR-KPP Attributes, Details, and Measures

Original Attribute from NR-KPP Description	Refined Attribute Details	Measures	Sample Data Sources	NR-KPP Component
Support net-centric military operations	Military Operations (e.g. mission areas or mission threads)	Effectiveness Measures used to determine success of the military operation	JMETLs and NMETLs	NR-KPP Effectiveness Measures
		Conditions under which the military operations must be executed		
	Operational tasks required by the military operations	Operational Performance Measures used to determine activity performance	JMETLs and NMETLs	NR-KPP Performance Measures
		Conditions under which the activity must be performed		
Enter and be managed in the network	Which networks do the net-centric military operations require	Operational Performance Measures for entering the network	N/A	NR-KPP Performance Measures
		Operational Performance Measures for being managed in the network		
Exchange Information	Information produced and consumed by each military operation and operational task	Operational Performance measures to ensure exchanges are: - Continuous - Survivable - Interoperable - Secure - Operationally Effective	DoDAF OV-3 Operational Information Exchange Matrix	NR-KPP Performance Measures

3.3.3 Net-Ready KPP Effectiveness and Performance Measures

The NR-KPP Compliance Statement specifies threshold performance measures in terms of satisfying all [applicable] joint critical operational activities, and objective performance measures in terms of satisfying all [applicable] operational activities. In other words, the system in question shall "enter and be managed" in the appropriate networks (attribute 2) and provide "effective information exchanges" (attribute 3) for all (objective) or all joint critical (threshold) operational activities the system supports (attribute 1). Numeric values for the objective/threshold of individual network entry/management MOPs, and associated information exchange MOPs are mathematically derived from the desired value of Mission Effectiveness associated with those operational activities. As indicated in the *Manual for the Operation of the Joint Capabilities Integration and Development System* (a.k.a. the JCIDS Manual)[15] (reference a) these values should be specified in the context of an overall operational scenario that describes the frequency and number of missions occurring at any given time. Programs can determine these values in a number of ways. The Mission Analysis and Information Analysis segments in Section 4 of the guidebook discuss this in more detail.

Note that Table 3-1 recommends data sources for two of the attributes from the refined NR-KPP. The data sources are recommended in part because they include measurable and testable metrics for each mission and Operational Task. Therefore incorporating those sources into the derived NR-KPP requirements will turn the NR-KPP into a measurable and testable KPP.

3.3.4 Net-Ready KPP Compliance Measures

The NR-KPP Compliance Statement contains five elements that make up the NR-KPP Compliance Measures. These elements are: Solution Architectures, Net-Centric Data and

[15] *Manual for the Operation of the Joint Capabilities Integration and Development System*, https://www.intelink.gov/wiki/JCIDS_Manual.

Services Strategy, Global Information Grid Technical Guidance, Information Assurance, and Supportability. These measures constrain the Systems Engineering Process used to support the acquisition of the system. For example, requiring DoDAF views constrains how programs provide traceability to show that the system meets its requirements. While testing for interoperability certification, the Joint Interoperability Test Command (JITC) evaluates a system's ability to meet the threshold and objective levels of these compliance measures. The NR-KPP's threshold and objective requirements have the same Compliance Measures. Unlike the NR-KPP Description and NR-KPP Effectiveness and Performance Measures, programs do not need to develop derived requirements for these NR-KPP Compliance Measures. Instead, programs should simply view the Compliance Measures as constraints on the Systems Engineering step in the Four-Step Process. The sections describing each of these steps in the Four-Step Process will discuss in more detail how these Compliance Measures constrain the Systems Engineering Process as well as how JITC verifies these measures.

Using the descriptions above, programs can now develop the derived NR-KPP requirements that make up the refined NR-KPP Compliance Statement shown in CJCSI 6212.01E, Enclosure E, Table E2. The refined NR-KPP Compliance Statement describes these derived requirements in terms similar to those used by other KPPs, and as a result makes it easier for programs to ensure their system satisfies the NR-KPP. Enclosure A includes a template view of the refined NR-KPP Compliance Statement. It should be emphasized that this refined NR-KPP Compliance Statement is simply a template that can be used use to capture the derived NR-KPP requirements and provide traceability back to the original NR-KPP Compliance Statement. It is in no way meant to replace the original NR-KPP Compliance Statement required by CJCSI 6212.01E (reference d).

4 Four-Step Net-Ready KPP Process

This section presents an overview of Four-Step Process that Program Managers, Systems Engineers, and Test Engineers can use to address the NR-KPP and effectively articulate their NR-KPP related efforts at Milestone and Gate Reviews. Figure 4-1 provides a graphical overview of the process flow and the NR-KPP attributes addressed at each step. The Four-Step Process includes the following activities:

1) Mission Level Systems Engineering Analysis
2) Information Analysis
3) Systems Engineering / Requirements Derivation
4) NR-KPP Documentation

Together, the *Mission Level Systems Engineering Analysis* step (abbreviated *Mission Analysis*) and *Information Analysis* step develop the refined NR-KPP Compliance Statement performance attributes. The *Systems Engineering / Requirements Development* step (abbreviated *Systems Engineering*) addresses the associated compliance measures and decomposes the derived NR-KPP into *system* performance requirements for use during system design and realization. The *NR-KPP Documentation* step discusses how the program manager uses the outcomes of the previous steps to develop the formal documentation products in which the NR-KPP is a mandated component, and ensures traceability of those products back to operational requirements.

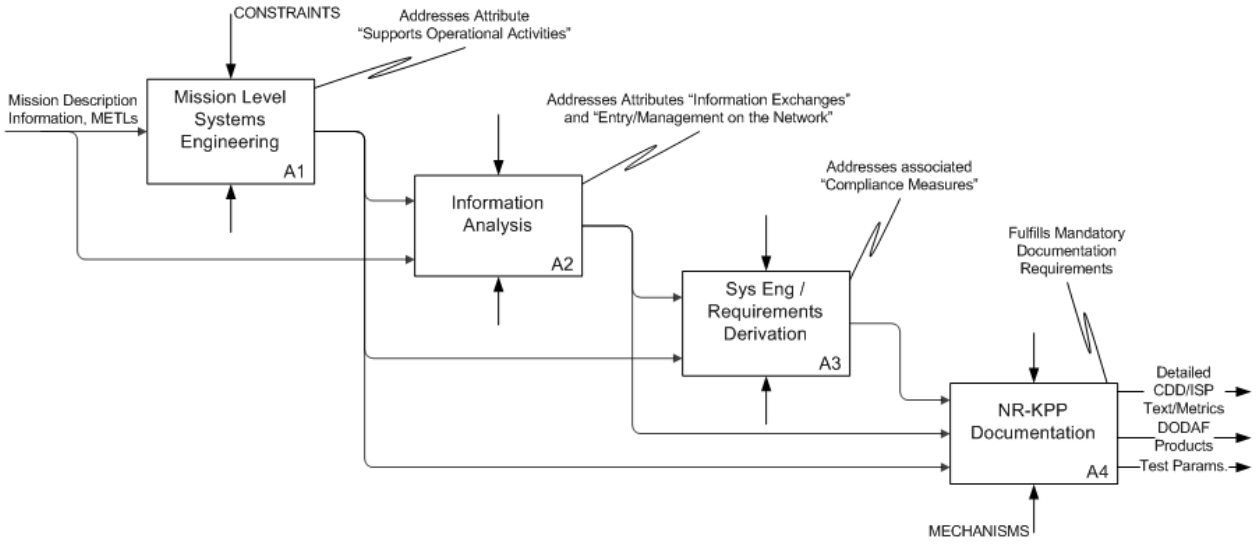


Figure 4-1: Overview of the NR-KPP Four Step Process

Ideally, the *Mission Analysis* and *Information Analysis* steps would take place during the Capabilities-Based Assessment (CBA) portion of the JCIDS process.[16] However, documentation from the CBA process may be insufficient to address the NR-KPP. This guide provides

[16] As stated in the *Manual for the Operation of the Joint Capabilities Integration and Development System*, the Capabilities Based Assessment (CBA) should identify the operational tasks, conditions, and operational performance standards needed to achieve desired mission outcomes.

information for programs that will be helpful to remedy these situations. This guide is not intended to provide an exhaustive tutorial on developing architecture products.

4.1 Mission Level Systems Engineering Analysis

4.1.1 Purpose

"Mission Analysis" for short, exposes the derived NR-KPP Operational Requirements in terms of missions, mission activities, and associated measures of *effectiveness* and *operational performance*. Figure 4-2 depicts the inputs, constraints, mechanisms and outputs relevant to the Mission Analysis step. It addresses the *Support Net-Centric Military Operations* attribute of the refined NR-KPP Compliance Statement. It validates the operational tasking developed during the Capability Based Assessment phase of the JCIDS process for the system. Even if the mission/tasking has been thoroughly developed during the CBA, this step allows the program of record to assimilate that tasking and fully understand the system information exchanges implications imposed by those operational requirements.

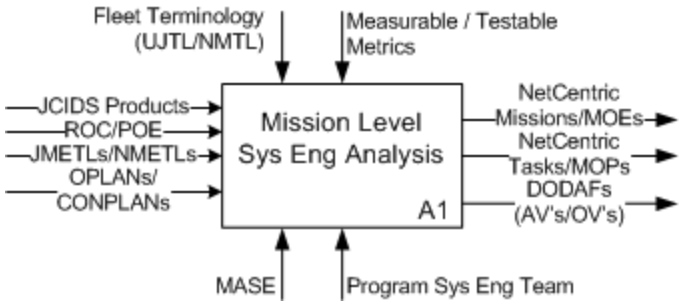


Figure 4-2: Mission Analysis

4.1.2 Key Points

As programs execute this step, they should keep a number of things in mind:

- Since the full catalog of enterprise level Mission Analyses have not been completed, some programs may find it difficult to find extensive artifacts in the DoD & Navy Architecture repositories that appropriately reflect their program of interest. (See process Inputs section below.)
- An exhaustive Mission Analysis examines elements outside the scope of an individual system. Therefore programs should work with the appropriate Community of Interest (COI) or Community of Practice (COP) to ensure coordination across systems and proper stakeholder involvement.
- Previous versions of the DoDAF architecture viewpoints lack ways to display some of the derived Operational Requirements and a mechanism to display Effectiveness Measures for the mission and Operational Performance Measures for the tasks. DoDAF version 2 has attempted to mitigate these omissions (e.g., allows augmenting the OV-5b with Operational Performance Metrics for each activity, and OV-6c activity models to be "executed" to assess overall mission thread performance).

4.1.3 Inputs

The DoD Architecture Registry System (DARS)[17] (reference l), Naval Architecture Repository System (NARS)[18] (reference n), or DoN Enterprise Architecture[19,20] repository (reference n) should contain the results of an applicable Mission Analysis. Any Mission Analysis results available from these three sources, or traceable authoritative analysis of military operations, should serve as the primary input to this step. Example documentation products may include the following.

- The program's JCIDS documentation[21] and/or JCIDS products from other relevant programs
- The Required Operational Capability/Projected Operating Environment (ROC/POE) for platforms that will field the system[22]
- Training requirements captured by Navy Mission Essential Task Lists (NMETLs) listed in the Navy Training Information Management System (NTIMS)[23] (reference o)
- Readiness reporting requirements captured in the JMETLs and NMETLs found in the Defense Readiness Reporting System (DRRS)[24] (reference p)
- Operational scenarios, operational plans (OPLANs) or contingency plans (CONPLANs) for near-term systems and Defense Planning Scenarios (DPS) for far-term systems

4.1.4 Constraints and Mechanisms

For this step, programs must specify the missions and Operational Tasks in terms the Fleet uses. Furthermore, the associated effectiveness and operational performance metrics need to be measurable and testable. The JMETL and NMETL frameworks provide a convenient way to articulate the NR-KPP requirements in measurable and testable terms used by the operational community. Collaboration with the operational community or knowledgeable representatives (e.g., Mission Area Systems Engineers) is strongly recommended.

The Program Office should collaborate with the Resource Sponsor to establish the level of derived requirements that are appropriate for the program and adjust the scope and resource allocation for the Mission Analysis accordingly. For the purposes of the NR-KPP, an abbreviated Mission Analysis is limited in scope to the operational tasking and associated performance measures allocated to the system(s) under development. Although this process will specifically focus on just those activities that are associated with information exchange, the entire scope of system activities will likely need to be examined in order to discern which activities are dependent on the information exchanges.

Exhaustive Mission Analysis begins with operational tasking that is completely system agnostic. It requires resourcing beyond the scope of a program office or single resource sponsor, however, it can also allow for development of the Operational Tasks, Operational Performance Measures, and Effectiveness Measures for the entire mission, and yield a better understanding of the trade-

[17] https://dars1.army.mil/IER2/
[18] https://nars.nswc.navy.mil/
[19] http://www.doncio.navy.mil/
[20] https://www.intelink.gov/wiki/DONEA
[21] Normally available through the JCPAT-E web-based application, on SIPRNET only
[22] OPNAV INSTRUCTION 3501 series documents, cataloged at http://doni.daps.dla.mil/allinstructions.aspx.
[23] NTIMS is also available as a web-based application on SIPRNET only.
[24] DRRS and service specific modules are also available as a web-based applications on SIPRNET only.

space available for materiel and non-materiel solutions. The analysis of an entire mission thread during the early JCIDS process should be considered a Navy Enterprise issue, with as much Community of Interest (COI) participation and review as possible. This would help ensure consistency of Mission Analysis products across multiple programs.

4.1.5 Outcomes

Initial documentation for this step may be as simple as a set of story-boards/scripts, schedule tables, or sequence diagrams. NR-KPP relevant outcomes should be similar regardless of whether the program conducts a thorough or abbreviated Mission Analysis, and should include:

- Critical and non-critical Operational Tasks required for the system under consideration.[25]
- Operational Effectiveness and Performance Measures for each task.

The intent is to specify the operational tasks and the serial/parallel sequence in which they are conducted, the reference mission conditions, and the MOEs/MOPs. The reference conditions can have a profound impact on the MOEs/MOPs and can include weather, darkness, restricted communications, or other common descriptors found in the UJTL and UNTL references. Pre-existing JCIDS products and DoDAF models may lack specifications for Measures of Effectiveness / Measures of Performance associated with the tasking. Measures of performance will generally be specified in directly measurable quantities such as numbers of personnel trained or numbers of targets disabled. Measures of Effectiveness will generally be specified in percentages, e.g., percent of unit trained or percent of opposing targets disabled.

A thorough Mission Analysis will also yield:

- An exhaustive list of critical and non-critical missions the system supports.[26]
- Effectiveness measures for each mission thread (e.g., probability of success).
- All critical and non-critical Operational Tasks required for each mission thread.[27] This differs from an abbreviated Mission Analysis in that it lists more than just those tasks required by the system under consideration.
- Operational Performance Measures for the additional tasking revealed.

The end product for this step will be a DoDAF-compliant activity model described through a series of (annotated) Operational Viewpoints. Programs should have the following DoDAF views available to demonstrate these derived requirements:

- An AV-1 to provide the context and scope of the missions a system supports.
- An OV-1 (or multiple OV-1s) to display the missions a system supports.
- An OV-4 to display the command hierarchy and external nodes needed for the mission. Although not required for the Mission Analysis, the NR-KPP documentation requires this view and it is best captured during the Mission Analysis.

[25] See Paragraph 4.c of Enclosure C to CJCSM 3500.03B. The list of joint critical mission/tasks vs. all operational tasks forms the basis for the Threshold and Objective values of the Net- Ready KPP.
[26] Ibid.
[27] Ibid.

- A partial OV-5b to display the activities in the mission. (The OV-5b will be completed during the next step, Information Analysis, to show the information each activity produces and consumes.
- An OV-6c to display the sequence of events/activities in the mission.
- An AV-2 to provide a dictionary of terms that are used in the architecture products.

The derived Operational Requirements produced by this step can be directly inserted into the template for the refined NR-KPP Compliance Statement included in Enclosure A. The NR-KPP template need only list Net-Ready Operational Tasks.

4.1.6 Process

Standardized processes for performing mission analyses can be found in documentation for the JMETL[28] and NMETL development manuals (reference q). Also, a more thorough Mission Thread Development Guidebook is in draft development by the DASN (RDT&E) CHSENG staff. System Engineers are strongly encouraged to use the Mission Thread Development Guide to perform this process step.

Missions, mission tasks, and associated effectiveness and performance measures for the system that have been developed in any of the preceding documentation can be extracted and included directly in the refined NR-KPP Compliance Statement. For any system specific tasking that has not been established in the preceding documentation, the following actions may be taken.

1) Talk through and write out a vignette / scenario for how the system will be used in the specific mission thread. (The AV-1 DoDAF product captures the information gleaned from this process in a standard format that can be easily archived and shared.) Participating entities (organizations and objects) are generally only described at the platform level; however, this process is being tailored to a specific system, thus deeper levels of detail are appropriate. The vignette should ultimately reflect a sub-set of one or more of the primary naval missions as described in the most recent revision of OPNAVINST C3501.2 (reference r).

2) Sketch out a picture of the vignette, graphically indicating the participating entities and the generic lines of lines of communication between them. (The DoDAF OV-1 provides a standardized format for capturing sharing this information.) Again, since the scope of this exercise is being tailored to a specific system acquisition, this Operational View should reflect a detail (subset) of an existing mission OV-1. Typically, only the communications end-points (information producer and consumer) are shown in this view.

3) Establish the entity/relationship model indicating the participating "manned" organizations and the information sharing relationships that occur between them. (The DoDAF OV-4 appropriately captures and represents this information in a nodes/connections network type diagram.) Intermediate information exchange nodes (e.g., chain of command relays) are appropriate to show in this view.

[28] See CJCSG 3501, The Joint Training Systems Primer, and the JMETL Development Handbook, located at http://www.dtic.mil/doctrine/training/trainingsystem.htm.

4) Establish the activities performed grouped by the organizations that perform them. (The OV-5 series of models captures several aspects of this information.) These activities should either directly reference a UJTL or UNTL tasking number, or represent an activity that is part of a UJTL/UNTL task. ***These activities must include a measure of effectiveness or measure of performance*** that can be mathematically transformed into a higher level measure of effectiveness. These MOEs/MOPs are used to derive the actual information exchange performance parameters associated with the NR-KPP.

5) Establish the series/parallel time sequencing of the activities, which may also be grouped by organization. (The OV-6 series of models captures this information.) Again, ***this view should include or be annotated with the associated Measures of Effectiveness / Measures of Performance.*** The advantage of capturing this information in an architectural model such as the DM2 is that the overall mission measure of effectiveness can be evaluated/re-evaluated depending on different resources, changing conditions, or changing technologies that are associated with executing the mission. These metrics enable the quantitative identification of design constraints and a rigorous engineering approach toward trade-space analysis of the system design.

6) Review the products collected thus far and establish a dictionary of terms, especially if terminology was needed to describe the operation that is not included in the higher level references (e.g., The UJTL). This dictionary of terminology comprises the initial AV-2, which may be updated in the subsequent steps.

4.2 Information Analysis

4.2.1 Purpose

Information Analysis determines the Information Exchange Requirements in terms of required networks and operational performance measures. Figure 4-3 depicts the inputs, constraints, mechanisms and outcomes of the Information Analysis step. The Information Analysis derives the attributes in the refined NR-KPP statement indicated by the phrases as ***Enter and Be Managed in the Network*** and ***Exchange Information***. Again, for the purposes of the NR-KPP, these attributes must be expressed in measurable and testable terms.

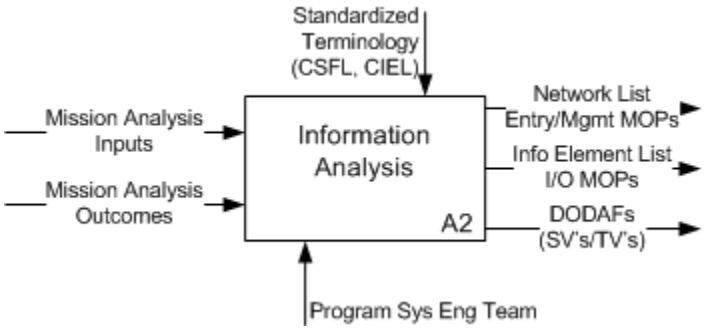


Figure 4-3, Information Analysis

4.2.2 Key Points

The Information Analysis step has essentially the same key points as the Mission Analysis, namely:

- The full catalog of enterprise level Information Analyses products have not likely been completed, thus extensive artifacts in the DoD & Navy Architecture repositories may be difficult to find.
- Programs should work with the appropriate Community of Interest (COI) or Community of Practice (COP) to ensure coordination to address Information Exchange Requirements outside the scope of an individual system. A list of COIs and their POCs can be found on the CES Metadata Registry homepage (reference s), in the left navigation column under "COI Directory".[29]
- Ensure operational performance metrics for the attributes discussed are included with the DoDAF artifacts.

4.2.3 Inputs

The primary inputs to the Information Analysis step are the outcomes of the Mission Analysis step (i.e., a model of operational tasking with measures of effectiveness and performance). Any directly applicable architectures or artifacts that were provided as inputs to the Mission Analysis step will also be useful.

4.2.4 Constraints

Programs will, to the greatest extent possible, make use of standardized lists to describe the Information Exchanges and Information Elements used in the mission thread. These standardized lists include the (Navy) Common Information Exchange List (CIEL)[30,31] (reference t), or the National Information Exchange Model (NIEM)[32] (reference u).

The Program Office should collaborate with the Resource Sponsor to establish the level of derived requirements that are appropriate, and adjust the scope and resource allocation accordingly. For the purposes of the NR-KPP, an abbreviated Information Analysis would be limited in scope to the Information Exchanges and measures of performance between the system(s) under development and external information sources or recipients. Although this process will specifically focus on those cross-boundary information exchanges, the entire scope of Information Exchanges associated with the mission thread will likely need to be examined in order to deal with Input / Output / Processing constraints, discoverability (future uses), and Information Assurance requirements.

The exhaustive information exchange analysis of an entire mission thread would be a Navy Enterprise issue; Program Offices should attempt to have as much Community of Interest (COI) participation and review as possible. This will help ensure consistency of Information Analyses across programs. Programs should also participate or stand up any interoperability meetings that address Information Elements produced or consumed by their system.

---

[29] CES Metadata Registry Website https://metadata.ces.mil/mdr/homepage.htm.
[30] The CIEL is referenced in the Naval Architecture Elements Reference Guide (NAERG), currently located on the SYSCOM Architecture Development and Integration Environment (SADIE) at https://sadie.spawar.navy.mil/.
[31] Additional information on the DON Enterprise Architecture can be found on the "Intelink" information portal at https://www.intelink.gov/wiki/DONEA.
[32] National Information Exchange Model http://www.niem.gov/

4.2.5 Outcomes

Outcomes of an abbreviated Information Analysis must include (threshold requirements):

- Information Elements produced or consumed by the (Net-Centric) Joint Critical Operational Tasks required for the system under consideration.
- Operational performance metrics for entry to and management in the network(s) that the system will connect to in support of those tasks.
- Operational performance metrics describing continuity, survivability, interoperability, security, and operational effectiveness associated with the Information Elements produced or consumed by the system under consideration.

Outcomes for an Information Analysis to meet the objective (all Net-Centric Operational Tasking) will also include the remainder of (all) operational tasking associated with the system's information exchanges, and the associated measures of performance for network entry and management for that tasking.

Outcomes of an in-depth Information Analysis would include:

- Network connections and information elements produced or consumed by all of the Net-Ready operational tasks required for each mission thread (***not just those tasks required by the system under consideration***).
- Operational performance metrics describing network entry and network management for the networks over which those information exchanges will be conducted.
- Operational performance metrics describing continuity, survivability, interoperability, security, and operational effectiveness for Information Elements produced or consumed during execution of the system.

These results essentially specify the system's derived Operational Information Requirements for each mission. Programs should use the following DoDAF views to document these requirements.

- An OV-2 should display a summary of the Information Elements produced and consumed, as annotations accompanying the need lines between operational nodes.
- An OV-3 should display the Information Elements produced and consumed along with their Operational Performance Measures.
- A full OV-5b should display each activity in the mission and the Information Elements produced and consumed by that activity.
- Although not present required, an OV-6a would be used to capture operational rules of engagement, such as "go silent under threat conditions" or restricted availability of resources / assets in specific operation areas.
- A DIV-2 (formerly the OV-7 in DoDAF v1.5) should display the Information Elements to start planning the program's data strategy.
- The required networks form the starting point for an SV-2.
- Programs should also continue developing the dictionary of terms used in these architecture products (i.e., update the AV-2).

Programs can also insert these derived Operational Information Requirements for the Net-Ready Operational Tasks into the template for the refined NR-KPP Compliance Statement included in

Enclosure A. The template only needs to include Information Requirements for Net-Ready Operational Tasks.

4.2.6 Process

Information Exchange Requirements that were appropriately developed during the Capabilities Based Assessment (CBA), and any program relevant documentation archived in the Defense or Navy Architecture Repository Systems (DARS/NARS) (references l & m) or program specific data archives, may extracted and directly included in the refined NR-KPP Compliance Statement.

For any information exchanges across the system boundary that have not been previously documented, the following actions may be taken.

1) For the operational tasking derived in the previous step, determine what information elements will be needed by the system to accomplish those tasks; also determine what information elements are produced by the tasking and if the information will be shared with an external system. These information exchanges can be ascertained from the OV-6 products, which are primarily intended to show the operating rules (OV-6a), and sequence and timing of activities (OV-6c), but are generally grouped by systems or organization and often depicted in a UML activity diagram. Whenever the scope of tasking crosses a system/organizational boundary or "swim-lane," there is generally a corresponding information exchange. These information exchanges can be documented as resource flows in the OV-2 and OV-3. Basic characteristics of the Information Elements that are being exchanged should be captured in the format of a Data Information Viewpoint conceptual model (DIV-1). As the information exchanges are further developed and details are fleshed out, the logical data model (DIV-2, formerly the OV-7) and physical data model (DIV-3, formerly the SV-11) can be built. In most cases, data information for the DIV-2 and DIV-3 will already be specified in higher level sources such as the NIEM or CIEL, commercial or military standards, or the interface control specifications / interface control documents of pre-existing acquisition systems.

2) Determine the services and systems that will participate in each of these information exchanges. These are the tools and resource being used by the organizations represented in the OV-2 that participate in the information exchanges. This information is best represented in the SvcV-1 model, and the SV-1 model.

3) Determine the communications paths or "networks" on which these services will be hosted. "Networks" in the context of the NR-KPP includes point-to-point communications links that create an information sharing "network" in support of the operational tasking. ***It is not limited in scope to the colloquial sense of multi-point communication via routed Internet Protocol (IP) data packets.*** This information will be represented by additional details on the SV-1.

4) Determine how the system will establish and maintain the communications interfaces listed. This will include measures of performance (e.g., how quickly) for how these interfaces are established, and may include parameters like refresh rates on credentials. This information will be captured in the SV-2 and DIV-2. A "sanity check" should be

performed at this point to determine if the expected measures of performance for these events, or constraints on those measures of performance, can and will support the measures of performance and measures of effectiveness established for the operational tasking captured in the OV models.

5) Determine the measures of performance required for the information exchanges themselves – e.g., latency, bandwidth/capacity and QoS/bit-error-rates. This information will be added to the DIV-2 and DIV-3. Again, determine if the proposed communications paths will be able to support the required information exchange performance parameters as determined by the operational tasking and captured in the OV models.

6) Determine the levels of information assurance that are required for each of the information exchanges. This includes all five aspects of information assurance: availability, authenticity, non-repudiation, integrity *and* confidentiality. This step is crucial for determining how the system will "enter and be managed" in the required networks. The information will also be added to the DIV-2 and DIV-3, and cross checked against the operational performance measures.

7) Review the products collected thus far and update the dictionary of terms (AV-2), especially if terminology was needed to describe the operation that is not included in the higher level references.

4.3 Systems Engineering / Requirements Derivation

4.3.1 Purpose

The primary purpose of the Systems Engineering / Requirements Derivation step (Systems Engineering for short) is to decompose the NR-KPP requirements from the Mission Analysis and Information Analysis into system performance requirements for use during system design and realization. This step is also needed to capture traceability to the standards and references cited in the compliance measures section of the refined NR-KPP Compliance Statement. Figure 4-4 below depicts the Systems Engineering step that is relevant to the NR-KPP requirements decomposition.

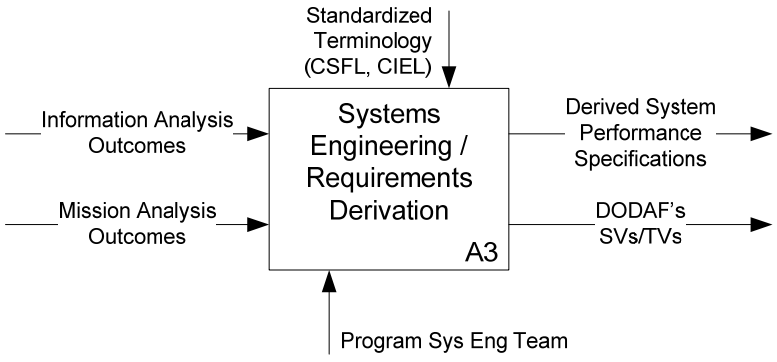


Figure 4-4: NR-KPP Systems Engineering / Requirements Derivation

4.3.2 Key Points

The following items are critically important to the success of the Systems Engineering / Requirements Development process.

- The derivation of system performance specifications cannot be properly accomplished without the measures of effectiveness and measures of performance information derived from the mission analysis.
- Likewise, the performance specifications for and information handling system cannot be appropriately derived without the clear understanding of the critical information elements and information exchange performance established through the Information Analysis step.
- The Joint Interoperability Test Command (JITC) has developed an NR-KPP Test Guidebook (reference v) that describes the process for evaluating a system's ability to meet the threshold and objective levels of the NR-KPP Compliance Measures.[33] Programs should review this guidebook to ensure their implementation of the process constraints will satisfy the JITC certification requirements.
- The DoDAF products used to display the Operational Systems and Systems Performance requirements will also form the basis of the Test Procedures used during Developmental, Operational and Joint Interoperability testing phases.

4.3.3 Inputs

The primary inputs to the Systems Engineering / Requirements Development step are the outcomes of the previous Mission Analysis and Information Analysis steps. Inputs are expected to be in the form of a multi-attribute Key Performance Parameter, with each attribute being expressed in terms of a measure of performance mathematically derivable from the tasking measures of performance / measures of effectiveness; the refined NR-KPP compliance statement template (Enclosure A) provides an example. Ideally, this information is also archived in the form of a DoDAF compliant architectural model. The model information is used in developing follow-on acquisition documentation and can be used to for checking consistency between interfacing systems.

4.3.4 Constraints

When executing this step, programs need to ensure the system complies with the five NR-KPP Compliance Measures given in the NR-KPP Compliance Statement for which the Joint Chiefs Instruction (CJCSI 6212.01E) (reference d) gives detailed procedures.

The DoDAF views should comply with DoDAF standards, DoD Information Enterprise Architecture (DIEA) business rules and principles, and DISR policies. DoDAF views produced throughout the NR-KPP development process should be consolidated with any applicable architecture documentation developed through other processes, and should also be registered in DARS (reference l).

Programs will, to the greatest extent possible, make use of standardized lists to describe the System Functions used accomplish the tasks/activities derived from the Mission Analysis, and for performing the information exchanges derived from the Information Analysis. These

[33] The JITC resource page, with links to the NR-KPP Testing Guidebook can be found at the following link https://www.intelink.gov/sites/jitc/default.aspx.

standardized lists include the Joint Common Systems Function List (JCSFL)[34] (reference k), as referenced in CJCSI 6212.01E (reference d).

In addition to the DoDAF representations, programs should use the Exposure Verification Tracking sheets, shown in CJCSI 6212.01E (reference d), to document compliance[35] of the system functions, system data exchanges, and data elements, with the Net-Centric Data Strategy, Net-Centric Services Strategy, and DoD Information Enterprise Architecture.

Where applicable, the logical interfaces documented in the SV-1, physical interfaces in the SV-2, and standards in the StdV-1 (formerly the TV-1) should comply with the Global Information Grid (GIG) Technical Profiles (GTPs) and/or GIG Key Interface Profiles (KIPs) until the GTPs have been exhaustively developed.

The system interfaces, functions and data exchanges should comply with IA requirements and specify the IA controls the system will use. These IA specifications can include Access Control, Availability, Confidentiality, Dissemination Control, Integrity, and Non-Repudiation Consumer/Producer.

Programs should specify derived spectrum and supportability requirements for each physical interface that uses the electromagnetic spectrum. Each physical interface and /or system function that uses the electromagnetic spectrum should comply with spectrum and supportability requirements to include Selective Availability Anti-Spoofing Module (SAASM) (reference w), Spectrum, and Joint Tactical Radio System (JTRS) requirements (reference x).

DoDAF products are not intended to document ALL system requirements. When necessary the standard products may be augmented with critically relevant information, but it is strongly advisable to conform to other commonly accepted standards for developing detailed requirements specifications (e.g., IEEE 1220) (reference y). The use of standards will facilitate identification of the necessary performance metrics.

The SE step should also result in derived IA and Supportability requirements. Programs should specify IA requirements used for each system function, interface, and system data exchange. These IA specifications can include Access Control, Availability, Confidentiality, Dissemination Control, Integrity, and Non-Repudiation Consumer/Producer.

Ultimately, the SE Process will turn these outcomes into a net-ready system design. The System Realization portion of the SE Process verifies the system's net-readiness. System Realization should develop procedures to verify and validate a system's net-readiness during Interoperability and Supportability (I&S) Certification.

[34] Information on the Joint Common Systems Function List is currently available at the following portal, under the auspices of USJFCOM J89, Standards and Policy branch: https://www.us.army.mil/suite/page/419489. The portal is part of the Defense Knowledge Online (DKO) resource portal and does require a login account.

[35] CJCSI 6212.01E exempts tactical systems, control systems, and weapons systems with time critical constraints from the requirement to demonstrate compliance with the data strategy.

The Design portion of the Systems Engineering Process ensures that derived NR-KPP requirements are decomposed into technical requirements for the system. The Realization portion of the SE Process ensures that system meets these technical requirements (to include I&S Certification). **The scope of the NR-KPP Systems Engineering Process Step is focused on deriving performance parameters for the system functions that occur as a result of Net-Ready Operational Tasking.**

4.3.5 Outcomes

The outcomes of the System Design portion of the SE step should include System Performance Requirements such as attributes, characteristics, functions, interfaces, information flows, and standards. Programs should display these technical requirements in the following DoDAF views as appropriate for the maturity of the system.

- An SV-1 should display the system's logical interfaces (e.g., what interfaces support the applications and services that produce data for or consume data from external systems).
- An SV-2 should display the system's physical interfaces (e.g., what interfaces support the system's physical connections to other systems).
- An SV-4 (formerly the SV-4a) should display the functions a system performs along with the data produced and consumed by each function.
- An SV-5a should display how the system's functionality supports the missions and Operational Tasks identified during the Mission Analysis (MA).
- An SV-6 should display the system data exchanges supporting the information flows identified during the Information Analysis and displayed in the OV-2, OV-3, and SV-4.
- The SV-7 will also display performance requirements for each the system data exchange.
- A DIV-3 (formerly the SV-11) should display the content of the system data exchanges identified in the SV-6. Because the SV-6 maps to the outcomes of the Information Analysis, the DIV-3 also displays the details of the Information Elements listed in the DIV-2. Information Assurance aspects will be capture in the DIV-3 and SV-7 as appropriate for the type of IA element and how it is related to the data/exchange.
- A StdV-1 (formerly TV-1) should display the standards used by the system interfaces in the SV-1 and SV-2, the system functions in the SV-4, the system data exchanges in the SV-6, and the system data in the DIV-3. A StdV-2 (formerly the TV-2) should display any expected changes in those standards, and any emerging standards under consideration for the future.
- Programs should update the dictionary of terms (AV-2) that they use in these architecture products.

In addition to DoDAF products, the programs should display the outcomes of the SE Process using (as applicable):

- Exposure Verification Tracking sheets shown in Appendix A to Enclosure E of CJCSI 6212.01E (reference d) to document the data a system produces and the services the system provides.

- GIG Technical Guidance (GTG) or GIG Technical Profile (GTP) compliance matrices managed by DISA.[36] (references z & aa)

4.3.6 Process

Chapter 4 of the Defense Acquisition Guidebook (DAG) provides a thorough treatment of the systems engineering process relevant to defense acquisition inclusive of decomposition of user requirements into system functions and performance parameters[37]. For the purposes of deriving system requirements associated strictly with the refined NR-KPP, the reader can perform the following steps.

1) Use the OV-5a & b, and the OV-6c viewpoints from the mission thread to determine the operational tasking that will be supported by the system under development. These tasks can be determined by examining the organizational node that will be using the system, and selecting the subset of tasking that node will perform, and/or derived from higher-level guidance provided by the resource sponsor. The SV-5a provides a mechanism for cataloging the system functions against the operational tasking they support. System functions should be selected from the Joint Common Systems Functions List (JCSFL) to the greatest extent possible. Where not possible, the architect should submit the appropriate change request against the JCSFL to include the "new" functionality.
2) Using an SV-4, identify the relationships / dependencies between the system functions listed in the SV-5a and the data produced and consumed by each function (listed in the DIV-2 & DIV-3).
3) Using an SV-7, catalog performance metrics for the system functions listed in the SV-4a. These metrics will be used throughout the system design and realization, to ensure the system performs as expected. An analysis of the SV-7 will help determine how well the system must perform to enable the specified task performance. This analysis provides the traceability between system performance and mission performance.
4) From the OV-3, OV-5a/b, OV-6c, and SV-5a, determine which nodes the system needs to exchange information with based on the Operational Tasks it supports. Identify the physical connections (e.g., Ethernet, SATCOM, Link 16, etc.) needed to support these information exchanges and display those physical interfaces in an SV-2.
5) Using an SV-6, identify the system data exchanges (resource flows) for the information produced or consumed by the system. An analysis of the SV-6 will help determine how well the system must perform the data exchanges to enable the specified task performance, again with the purpose of providing traceability between the system performance and the required mission performance.
6) Using a DIV-3 (Physical Data Model – formerly the SV-11) define the structure of each system data exchange in the SV-6. The textual description of the DIV-3 is also used to answer questions related to storage of the data and metadata, including but not limited to data/meta-data storage locations, persistence, registries and discoverability, etc. Again,

[36] GTG: < https://www.intelink.gov/wiki/Portal:GIG_Technical_Guidance
GTPs: https://www.intelink.gov/wiki/Portal:GIG_Technical_Guidance/GTG_GTPs/GTP_Development_List
[37] https://dag.dau.mil/Pages/Default.aspx

the DoDAF products should provide traceability between the Information Elements specified and related in the OV-3, OV-5a/b, and DIV-2 (formerly the OV-7) and the system functions and data exchanges specified in the SV-4a, SV-5a, SV-6, and DIV-3.

7) Although not required at the time of this writing, the Service View (SvcV-x) products defined by the DoDAF should also be used to describe logical services provided by the system that produce information for another node or consume information from another node. This information facilitates modeling and simulation of the system and planning for the Navy's enterprise data strategy.

8) Use the StdV-1 (formerly the TV-1) to catalog standards used by the logical interfaces in the SV-1, the physical interfaces in the SV-2, the system functions in the SV-4a, and the data exchanges in the SV-6. A StdV-2 (formerly the TV-2) will be used to catalog emerging or expected changes in those standards.

9) Examine the DoD Metadata Registry (MDR) (reference bb) or Net-Centric Enterprise Services (NCES) Service Registry (reference cc) to see if either repository contains data or service strategies the program can reuse. If no such strategies exist, notify the Data or Service Portfolio Manager that the program will develop and provide recommendations for strategies required by the program. Ask the Portfolio Manager with whom they should coordinate in order to have their strategies approved and become the standard in the Data or Service Repository.

10) Develop the necessary data/services strategy and publish in the appropriate registry.

11) Review the products collected thus far and update the dictionary of terms (AV-2), especially if terminology was needed to describe the operation that is not included in the higher level references.

4.4 Documentation

4.4.1 Purpose

The primary purpose of the Documentation step consolidates and prepares the information specifying the NR-KPP into required formats, and incorporates the completed NR-KPP into the Acquisition Documentation that it is intended to support (e.g., the JCIDS capability documents and the Information Support Plan). It also provides formal traceability between the Operational Requirements in the original NR-KPP Compliance Statement, derived requirements in the refined NR-KPP Compliance statement, and system design. The step is also intended to provide a standardized framework to document the system's net-ready aspects that can be included in the system specification, contract specification, as well as the system test and evaluation (verification/validation) processes. Figure 4-5 depicts the inputs, constraints, mechanisms and outcomes of the NR-KPP Documentation step.

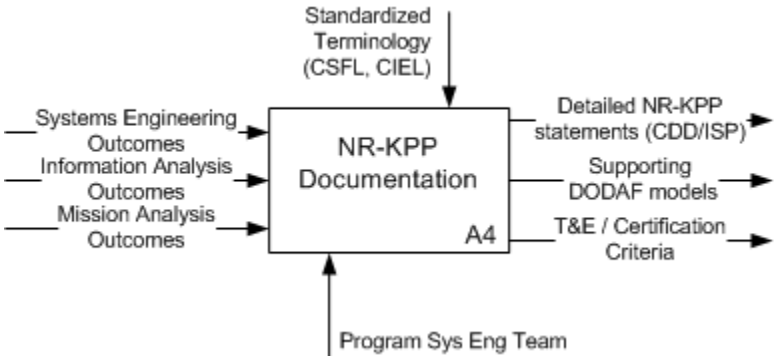


Figure 4-5, Documenting the NR-KPP

4.4.2 Key Points

The following items are critically important to the success of the Systems Engineering / Requirements Development process.

- The NR-KPP exists principally as an element of the Joint Capability Integration and Development System (JCIDS)[38] (reference a) and Joint Interoperability & Supportability (I&S) Certification[39] processes (reference d). The NR-KPP appears in the acquisition program's Capability Development or Capability Production Document. A copy appears in the Information Support Plan and may include updates, additional details, or references to derived requirements.
- Programs are mandated to provide supplemental system architecture information addressing the NR-KPP in the form of DoDAF viewpoint products in appendices to both the Capability Development/Production Document (CDD or CPD) and the Information Support Plan (ISP).
- Programs may have to augment existing DoDAF products (e.g., the OV-5a/b) to associate operational performance metrics with each task to indicate the performance traceability between the system and the mission it supports.
- The information system related requirements listed in the System Design Specifications and Test & Evaluation Plans should be explicitly traceable to the NR-KPP documented in the CDD/CPD and ISP.

4.4.3 Inputs

The primary inputs to the NR-KPP Documentation Development step are the outcomes of the previous Systems Engineering / Requirements Development step, but will include information directly produced by the Mission Analysis and Information Analysis steps.

4.4.4 Constraints

As indicated in the NR-KPP Compliance Measures, programs need to document the results in terms of DoDAF views, Exposure Verification Tracking Sheets (a.k.a. "Blue Sheets"), and GIG Technical Profile (GTP) compliance matrices.

As with the previous steps, the documentation products described here would normally be produced as part of the JCIDS process, however, due to the issues discussed previously, the information may not have been completely developed or appropriately registered. By delegation

[38] CJCSI 3170.01; G is the current revision at the time of this writing.
[39] CJCSI 6212.01; E is the current revision at the time of this writing.

or by default, producing this documentation in the appropriate formats and vetting though the appropriate processes, may have become the responsibility of the managing program office.

4.4.5 Outcomes

The outcomes of the Documentation step should capture the system's derived Operational Requirements and System Performance Requirements in accordance with the definition of a Key Performance Parameter as provided by CJCSI 3170.01G (reference a) and the corresponding JCIDS Process Manual. Attributes and formats specific to the Net Ready Key Performance Parameter as given by CJCSI 6212.01E (reference d) should also be included. A brief summary of these products are as follows:

- A verbatim inclusion of the Net Ready Key Performance Parameter Compliance Statement
- Textual description of the NR-KPP attributes and associated measures of performance and supportability (for inclusion in the CDD/CPD sections 6 and 8 respectively, and Net Centricity section of the EISP).
- The following matrix, Figure 4-6, reproduced from CJCSI 6212.01E, Enclosure E, table E-1 indicates the supplementary artifacts and architectural products required. Note that the artifacts are named by Mnemonic and full title according to the DoDAF v1.5 naming convention, however as the table indicates, these have changed for DoDAF v2.0. A complete crosswalk of the DoDAF v1.5 to DoDAF v2.0 products is available on the DoDAF resource page hosted by the DoD CIO[40] (reference e).

Document	Supportability Compliance	DOD Enterprise Architecture Products (IAW DODAF) (see Note 5)																Data/Service Exposure Sheets	IA Compliance	GTG Compliance
		AV-1 /AV-2	OV-1	OV-2	OV-3	OV-4	OV-5	OV-6C	OV-7	SV-1	SV-2	SV-4	SV-5	SV-6	SV-11	TV-1	TV-2			
ICD			X																	
CDD	X	3	X	X	X	X	X	X			X	X	X	X		2	2	1	X	X
CPD	X	3	X	X	X	X	X	X	1		X	X	X	X	1	2	2	1	X	X
ISP	X	3	X	X	X	X	X	X	4		X	X	X	X	4	2	2	1	X	X
TISP	X	3	X		X		X	X		X			X	X		2	2	1	X	X
ISP Annex (Svcs/ Apps)	X	3	X				X				X	X	X	X		2	2	1	X	X
X		Required (PM needs to check with their Component for any additional architectural/regulatory requirements for CDDs, CPDs, ISPs/TISPs. (e.g., HQDA requires the SV-10c)																		
Note 1		Required only when IT and NSS collects, processes, or uses any shared data or when IT and NSS exposes, consumes or implements shared services,																		
Note 2		The TV-1 and TV-2 are built using the DISRonline and must be posted for compliance.																		
Note 3		The AV-1 must be uploaded onto DARS and must be registered in DARS for compliance																		
Note 4		Only required for Milestone C, if applicable (see Note 1)																		
Note 5		The naming of the architecture views is expected to change with the release of DODAF v2.0 (e.g., StdV, SvcV, StdV, DIV). The requirements of this matrix will not change.																		

Figure 4-6, Required Architecture Products to Address the NR-KPP

Programs should register or publish these NR-KPP artifacts to DARS, NARS, and/or the DoD Information Technology Standards Registry (DISR) (references l, m, n, dd) as appropriate, and ensure the program's requirements documents include references/links to these artifacts, as applicable.

[40] The DoDAF 2 Resource Page can be found at the following URL http://cio-nii.defense.gov/sites/dodaf20/.

4.4.6 Process

The JCIDS Process Manual[41] (reference a) provides basic direction and templates for preparing the Capability Development Document / Capability Production Document inclusive of the NR-KPP. The Defense Acquisition Guidebook (DAG), Chapter 7, section 7.3.6[42] (reference ee) contains directions & guidance for developing the program's Information Support Plan.

For CDD [CPD] development, section 6, System Capabilities Required (paraphrased from the JCIDS manual):

1) Provide a description of each attribute of the NR-KPP in individual paragraphs (one per attribute). Use the integrated architecture products developed previously as the primary source material for these descriptions. (These products will be appended to the capability document.) Include a supporting rationale for the capability and cite any existing analytic references. Present each attribute in output-oriented, measurable and testable terms and provide a threshold and an objective value. Explicitly indicate if the objective and the threshold values are the same by including the statement "Threshold = Objective."
2) Discuss the operating environment/conditions as appropriate; and any additional information that the PM should consider.
3) If the Capabilities Document is describing a System-of-Systems solution, it must describe the attributes for the System-of-Systems level of performance and any unique attributes for each of the constituent systems.
4) If the CDD is being used to describe multiple increments, clearly identify which attributes apply to each increment. If the attribute threshold values change between increments, clearly identify the threshold for each increment.
5) Provide a table summarizing the NR-KPP attributes in threshold/objective format, as depicted below. Correlate each attribute to the capability defined in the ICD and the Tier 1 and 2 JCAs to which they contribute directly. (The table can be captured in an appendix to the capability document.)

Table 4-1: Example Key Performance Parameter Table

JCA Tier 1/2	Key Performance Parameter (attribute)	Development Threshold	Development Objective
	KPP 1	Value	Value
	KPP 2	Value	Value
	KPP 3	Value	Value

[41] *Manual for the Operation of the Joint Capabilities Integration and Development System,* https://www.intelink.gov/wiki/JCIDS_Manual.
[42] Defense Acquisition Guidebook (DAG) CH7.3.6, ISPs, EISPs & TISPs https://acc.dau.mil/CommunityBrowser.aspx?id=334031&lang=en-US.

For CDD [CPD] development, section 8, IT & NSS Supportability:

6) Provide an estimate of the expected bandwidth and quality of service requirements for support of the capability (on either a per-unit or an aggregate basis, as appropriate). This description must explicitly distinguish between support acquired as part of this program, and support provided through other systems or programs.
7) The sponsor must identify the communities of interest with which they are working to make the capability's data secure, visible, accessible, and understandable to other users on the Global Information Grid.

For the Traditional ISP Document, Defense Acquisition Guide, Chapter 7.3.6.7 details an explicit thirteen (13) step ISP development procedure[43] (reference ee). Information required for the 13 step procedure will be gleaned directly from the integrated architecture products and the textual descriptions developed for the capabilities documents. The information covered by the 13 step procedure addresses the elements of the Net Ready KPP, however element that are specifically part of the NR-KPP should state so, and cite the capability document or architecture product from which they were derived.

For inclusion in the Enhanced ISP (electronic): The EISP tool prompts the user for information according to a procedure equivalent to the document version. The primary difference between the two types of ISPs is in how the data is stored and made searchable, linkable and available for reuse by other programs in the EISP tool. See section 7.3.6.8 of the Defense Acquisition Guide[44] (reference ee).

[43] DAG CH7.3.6.7, ISP contents https://acc.dau.mil/CommunityBrowser.aspx?id=334031&lang=en-US.
[44] DAG CH7.3.6.8, EISP contents https://acc.dau.mil/CommunityBrowser.aspx?id=334040.

ENCLOSURE A
NR-KPP TEMPLATE

Using the descriptions given in this Guidebook, programs can refine the standard NR-KPP Compliance Statement given in CJCSI 6212.01E to develop derived NR-KPP requirements. These derived requirements describes the NR-KPP in terms similar to those used by other KPPs, and as a result makes it easier for programs to implement standard systems engineering (SE) process to ensure their system satisfies the NR-KPP. Figure A1 below illustrates a template for this refined NR-KPP Compliance Statement.

KPP		Threshold (T)	Objective (O)
Support Net-Centric Military Operations			
		Effectiveness Measures	**Effectiveness Measures**
Missions			
Mission 1	Effectiveness Measure	Value	Value
	Conditions		
Mission 2	Effectiveness Measure	Not Critical	Value
…	Conditions		
		Performance Measures	**Performance Measures**
Operational Tasks			
Task 1	Operational Performance Measure	Value	Value
	Conditions		
Task 2	Operational Performance Measure	Not Critical	Value
…	Conditions		
Enter and Be Managed In the Network			
Network 1	Network Entry Performance Measure	Value	Value
	Network Mgmt. Performance Measure	Value	Value
Network 2	Network Entry Performance Measure	Doesn't support a critical activity	Value
…	Network Mgmt. Performance Measure	Doesn't support a critical activity	Value
Exchange Information			
Information Element 1	Continuity Measure	Value	Value
	Survivability Measure	Value	Value
	Interoperability Measure	Value	Value
	Security Measure	Value	Value
	Operational Performance Measure	Value	Value
Information Element 2	Continuity Measure	Doesn't support a critical activity	Value
	Survivability Measure	Doesn't support a critical activity	Value
	Interoperability Measure	Doesn't support a critical activity	Value
	Security Measure	Doesn't support a critical activity	Value
	Operational Performance Measure	Doesn't support a critical activity	Value
		Compliance Measures	**Compliance Measures**
		DoD EA	DoD EA
		Net-Centric Data/Services Strategy	Net-Centric Data/Services Strategy
		GTG and GESPs	GTG and GESPs
		Information Assurance	Information Assurance
		Supportability	Supportability

Figure A-1. Refined NR-KPP Compliance Statement

ENCLOSURE B
GLOSSARY AND LIST OF ACRONYMS

List of Terms and Definitions

Attributes – A quantitative or qualitative characteristic of an element or its actions. Defined in CJCSI 3170.01G.

Capability – The ability to achieve a desired effect under specified **standards** and **conditions** through combinations of means and ways across the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) to perform a set of **tasks** to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms in the format of an initial capabilities document or a joint DOTMLPF change recommendation. In the case of materiel proposals/documents, the definition will progressively evolve to DOTMLPF performance attributes identified in the capability development document and the capability production document. Defined in CJCSI 3170.01G.

KPP – Those capabilities or characteristics considered essential for successful mission accomplishment. Failure to meet a system or program's KPP threshold can be cause for the concept or system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a system or program's KPP threshold can be cause for the family-of-systems or system-of-systems concept to be reassessed or the contributions of the individual systems to be reassessed. KPPs are validated by the Joint Requirement Oversight Council (JROC). KPPs are included in the acquisition program baseline. Defined in CJCSI 6212.01E.

Mission – A mission can be defined in four ways: 1. The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore; 2. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task; 3. An assignment with a purpose that clearly indicates the action to be taken and the reason therefore; 4. The dispatching of one or more aircraft to one particular task. Defined in CJCSM 3500.03B.

Mission Essential Task List – A list of joint mission-essential tasks selected by a commander to accomplish an assigned or anticipated mission. A joint mission-essential task list includes associated tasks, conditions, and standards and requires the identification of command-linked and supporting tasks. Defined in CJCSM 3500.03B.

Mission Systems Engineering – A process for conducting Systems Engineering that is based on the principle that Operational Requirements are defined by missions (and their associated Operational Tasks) that war-fighters must perform.

Mission Thread – A specific sequence of tasks performed by operational nodes to accomplish a mission in a given scenario.

Net-Centric Military Operations – The military exploitation of the human and technical networking of all elements of an appropriately trained joint force by fully integrating collective

capabilities, awareness, knowledge, experience, and superior decision making to achieve a high level of agility and effectiveness in dispersed, decentralized, dynamic and uncertain military operational environments. Adapted from the definition in Net-Centric Environment JFC, v1.0, 7 April 2005.

Net-Ready – This Guidebook uses the following abbreviated definition of net-readiness: A net-ready system meets the requirements for both the technical exchange of information and the operational effectiveness of those exchanges. These requirements include information needs, information timeliness, IA accreditation, and Net-ready attributes.

The full definition of net-readiness is given by CJCSI 6212.01E as follows: DOD IT and NSS that meets required information needs, information timeliness requirements, has IA accreditation, and meets the attributes required for both the technical exchange of information and the operational effectiveness of that exchange. DOD IT and NSS that is Net-Ready enables warfighters and DOD business operators to exercise control over enterprise information and services through a loosely coupled, distributed infrastructure that leverages service modularity, multimedia connectivity, metadata, and collaboration to provide an environment that promotes unifying actions among all participants. Net-readiness requires that IT and NSS operate in an environment where there exists a distributed information processing environment in which applications are integrated; applications and data independent of hardware are integrated; information transfer capabilities exist to ensure communications within and across diverse media; information is in a common format with a common meaning; there exist common human computer interfaces for users; and there exists effective means to protect the information. Net-Readiness is critical to achieving the envisioned objective of a cost-effective integrated environment. Achieving and maintaining this vision requires interoperability:

a) Within a Joint Task Force/combatant command area of responsibility (AOR).
b) Across combatant command AOR boundaries.
c) Between strategic and tactical systems.
d) Within and across Services and agencies.
e) From the battlefield to the sustaining base.
f) Among U.S., Allied, and Coalition forces.
g) Across current and future systems.

Net-Ready Operational Task – An Operational Task that produces information for an external system or consumes information from an external system.

Node – Operational unit (e.g. ship, submarine, airplane, shore site, etc.) that can perform an Operational Task.

NR-KPP Attributes – The three attributes listed in the NR-KPP Description that are used to determine if a system satisfies the NR-KPP. These attributes are: support net-centric military operations, enter and be managed in the network, and exchange information. These are the same thing as net-ready attributes. Defined in CJCSI 6212.01E.

NR-KPP Compliance Measures – The five process constraints listed in the NR-KPP Compliance Statement. These constraints were summarized earlier in the Guidebook. Their full definition is as follows: 1) Solution architecture products compliant with DOD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges; 2) Compliant with Net -Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DOD Information Enterprise Architecture (DOD IEA), excepting tactical and non-IP communications; 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DOD Enterprise Architecture and solution architecture views; 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization To Operate (ATO) by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements. Defined in CJCSI 6212.01E.

NR-KPP Compliance Statement – Template used to capture the NR-KPP Definition. The NR-KPP Compliance Statement must be included in a system's CDD, CPD, and ISP. The Guidebook recommends that programs refine the NR-KPP Compliance Statement to more clearly identify the NR-KPP's Operational Requirements. Defined in CJCSI 6212.01E.

NR-KPP – Guidebook uses the following abbreviated definition of the NR-KPP: The NR-KPP is a key parameter stating a system's operational requirements for information, the timeliness of that information, Information Assurance (IA), and net-ready attributes for both the technical exchange of information and the operational effectiveness of that exchange. CJCSI 6212.01E articulates this definition in terms of an NR-KPP Compliance Statement. To satisfy the NR-KPP, programs must show that they completely satisfy the capability's information needs in a timely and accurate manner.

The full definition of net-readiness is given by CJCSI 6212.01E as follows: The NR-KPP is a key parameter stating a system's information needs, information timeliness, IA, and net-ready attributes required for both the technical exchange of information needs, information timeliness, IA, and net-ready attributes required for both the technical exchange of information and the operational effectiveness of that exchange. The NR-KPP consists of information required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is composed of the following elements: 1) Compliant solution architecture, 2) compliance with DOD Net-centric Data and Services strategies, including data and services exposure criteria, 3) compliant with applicable GIG Technical Direction to include DISR mandated IT Standards reflected in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DOD Information Enterprise Architecture and solution architecture system/service views, 4) verification of compliance with DOD IA requirements, and 5) compliance with Supportability elements to include SAASM and the JTRS.

NR-KPP Description – Portion of the NR-KPP Compliance Statement that describes the NR-KPP Attributes. The Guidebook uses a summarized version of the NR-KPP Description. The

full description is as follows: The capability, system, and/or service must support Net-Centric military operations. The capability, system, and/or service must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The capability, system, and/or service must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability. Defined in CJCSI 6212.01E.

NR-KPP Effectiveness and Performance Measures- Portion of the NR-KPP that describes the measurable and testable Operational Requirements for the NR-KPP. These Operational Requirements are the Threshold and Objective performance values for each of the NR-KPP Attributes. The full description from the NR-KPP Compliance Statement is as follows: The capability, system, and/or service must fully support execution of joint critical operational activities and information exchanges identified in the DOD Enterprise Architecture and solution architectures based on integrated DODAF content. Defined in CJCSI 6212.01E.

Operational Performance Requirements – a User- or user representative-generated validated needs developed to address mission area deficiencies, evolving threats, emerging technologies, or weapon system cost improvements. Operational requirements form the foundation for weapon system-unique specifications and contract requirements. Defined in the Glossary of Defense Acquisition Acronyms & Terms, 12th Edition, July 2005. The NR-KPP's Operational Performance Requirements are the NR-KPP Effectiveness and Performance Measures and the NR-KPP Compliance Measures.

Refined NR-KPP– A modification of the original NR-KPP that more clearly identifies the NR-KPP's Operational Requirements. This refined NR-KPP is captured in the refined NR-KPP Compliance Statement shown in Enclosure A.

System Design – The portion of the Systems Engineering Process used for top-down design. This part of Systems Engineering ultimately develops various detailed specifications and other products that describe system solutions. System Design includes the System Engineering Technical Processes of Requirements Development, Logical Analysis, and Design Solution. Defined in Defense Acquisition Course SYS 101.

System Performance Requirements – Performance requirements the system must meet in order to satisfy its Operational Requirements.

System Realization – Providing the physical design solution in a product form suitable for meeting the applicable acquisition phase exit criteria, including product verification and validation and transitioning the product to the next level up of the system structure or ultimately, to the customer. System Realization includes the Systems Engineering Technical Processes of Implementation, Integration, Verification, Validation, and Transition**.** Defined in Defense Acquisition Course SYS 101.

Systems Engineering Process – The overarching process that a program team applies to transition from a stated capability need to an operationally effective and suitable system. Systems engineering encompasses the application of systems engineering processes across the

acquisition life cycle (adapted to each and every phase) and is intended to be the integrating mechanism for balanced solutions addressing capability needs, design considerations and constraints, as well as limitations imposed by technology, budget, and schedule. The systems engineering processes are applied early in concept definition, and then continuously throughout the total life cycle. Defined in the Defense Acquisition Guidebook.

List of Acronyms & Abbreviations

ASN	Assistant Secretary of the Navy
ATO	Authority To Operate
AV	(DoDAF) All Viewpoint
C4I	Command, Control, Communications, Computers, Intelligence
CBA	Capabilities-Based Assessment
CDD	Capability Development Document
CHSENG	Chief Systems Engineer
CIEL	Common Information Elements List
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COI	Community of Interest
CONPLAN	Contingency Plan
COP	Community of Practice
CPD	Capability Production Document
DAG	Defense Acquisition Guidebook
DARS	DoD Architecture Registry System
DASN	Deputy Assistant Secretary of the Navy
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DIEA	DoD Information Enterprise Architecture
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DIV	(DoDAF) Data and Information Viewpoint
DM2	DoDAF Meta-Model
DOTMLPF	Doctrine, Organizations, Training, Materiel, Leadership, Personnel, and Facilities
DPS	Defense Planning Scenario
DRRS	Defense Readiness Reporting System
GESP	GIG Enterprise Service Profile
GIG	Global Information Grid
GTG	GIG Technical Guidance
GTP	GIG Technical Profile
I&S	Interoperability and Supportability
IA	Information Assurance
IATO	Interim Authority To Operate
ICD	Initial Capabilities Document
IEEE	Institute of Electrical and Electronics Engineers
IER	Information Exchange Requirement

IP	Internet Protocol
ISP	Information Support Plan
IT	Information Technology
JCA	Joint Capabilities Area
JCIDS	Joint Capabilities Integration and Development System
JCSFL	Joint Common Systems Function List
JITC	Joint Interoperability Test Command
JMETL	Joint Mission Essential Task List
JROC	Joint Requirements Oversight Council
JTRS	Joint Tactical Radio System
KIP	Key Interface Profiles
MA	Mission Analysis
MDR	Metadata Registry
MOE	Measure of Effectiveness
MOP	Measure of Performance
NARS	Naval Architecture Repository System
NCES	Net-Centric Enterprise Services
NMETL	Navy Mission Essential Task List
NR-KPP	Net-Ready Key Performance Parameter
NSERC	Naval Systems Engineering Resource Center
NSS	National Security Systems
NTIMS	Navy Training Information Management System
OPLAN	Operational Plan
OT&E	Operational Test and Evaluation
OV	(DoDAF) Operational Viewpoint
RD&A	Research, Development, and Acquisition
RDT&E	Research, Development, Test, and Evaluation
ROC/POE	Required Operational Capability/Projected Operating Environment
SAASM	Selective Availability Anti-Spoofing Module
SE	Systems Engineering
SV	(DoDAF) Systems Viewpoint
StdV	(DoDAF) Standards Viewpoint
SvcV	(DoDAF) Services Viewpoint
TV	(DoDAF) Technical View (obsolete)
UJTL	Universal Joint Task List
UNTL	Universal Navy Task List