CLASSIFICATION (U)

2006 PEO/SYSCOM Conference

Net Ready Key Performance Parameter

A Practical Approach

COL Brian P. Hamilton

Chief, Information Integration Division, J6, The Joint Staff

7 & 8 November 2006

16th Chairman's Priorities

- **Win the War on Terrorism**
- **Accelerate Transformation**
- **Strengthen Joint Warfighting**
- **Improve the Quality of Life of our Service Members and our Families**

The Joint Staff will be an agile, empowered, innovative and results oriented organization supporting CJCS in the execution of his duties as the Principal Military Advisor to the President of the United States, the Secretary of Defense and the National Security Council

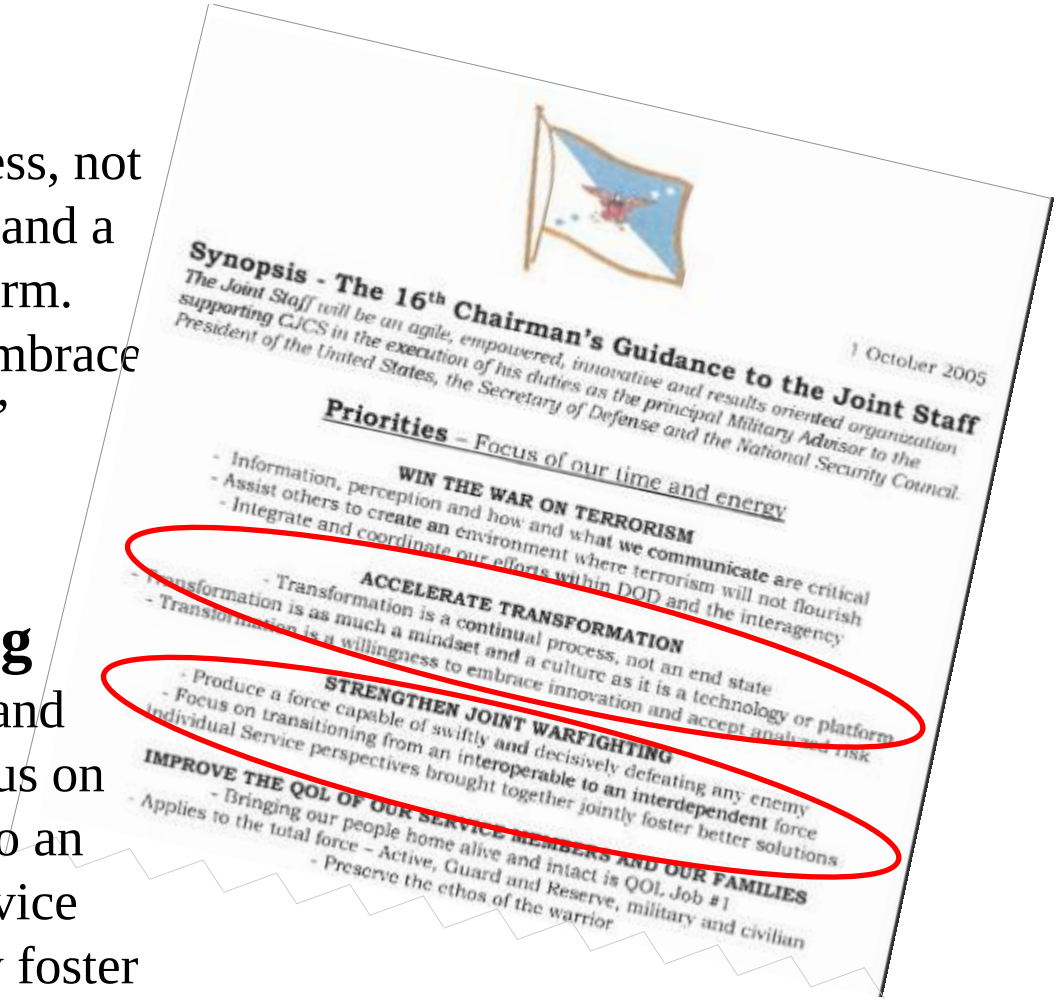
Chairman's Priorities

Accelerate Transformation

"Transformation is a continual process, not an end state; it is as much a mindset and a culture as it is a technology or platform. Transformation is a willingness to embrace innovation and accept analyzed risk"

Strengthen Joint Warfighting

"Produce a force capable of swiftly and decisively defeating any enemy; focus on transitioning from an interoperable to an interdependent force; individual Service perspectives brought together jointly foster better solutions"



Synopsis - The 16th Chairman's Guidance to the Joint Staff

1 October 2005

The Joint Staff will be an agile, empowered, innovative and results oriented organization supporting CJCS in the execution of his duties as the principal Military Advisor to the President of the United States, the Secretary of Defense and the National Security Council.

Priorities – Focus of our time and energy

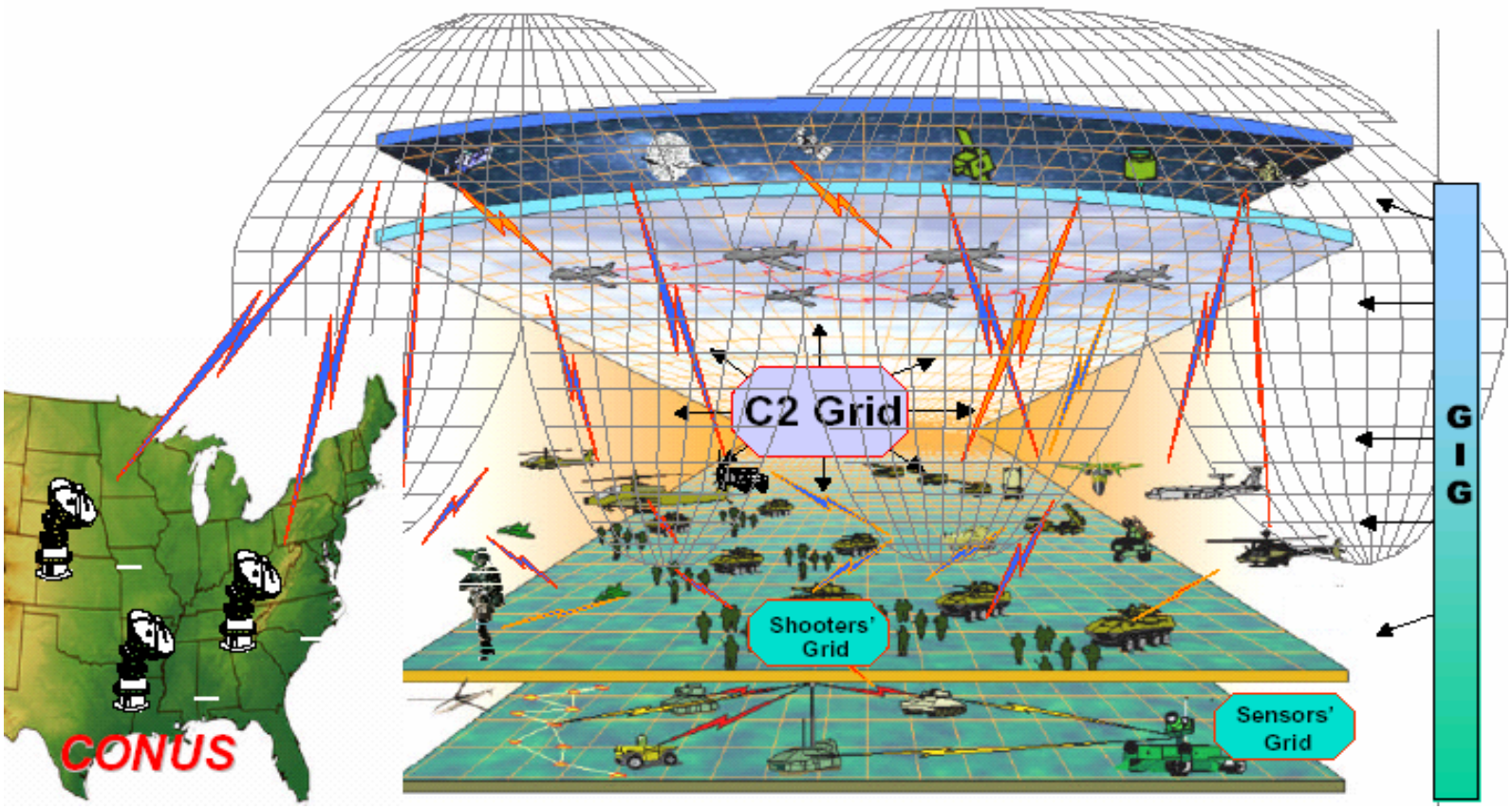
WIN THE WAR ON TERRORISM
- Information, perception and how and what we communicate are critical
- Assist others to create an environment where terrorism will not flourish
- Integrate and coordinate our efforts within DOD and the interagency

ACCELERATE TRANSFORMATION
- Transformation is a continual process, not an end state
- Transformation is as much a mindset and a culture as it is a technology or platform
- Transformation is a willingness to embrace innovation and accept analyzed risk

STRENGTHEN JOINT WARFIGHTING
- Produce a force capable of swiftly and decisively defeating any enemy
- Focus on transitioning from an interoperable to an interdependent force
- Individual Service perspectives brought together jointly foster better solutions

IMPROVE THE QOL OF OUR SERVICE MEMBERS AND OUR FAMILIES
- Bringing our people home alive and intact is QOL Job #1
- Applies to the total force – Active, Guard and Reserve, military and civilian
- Preserve the ethos of the warrior

The Global Information Grid (GIG)

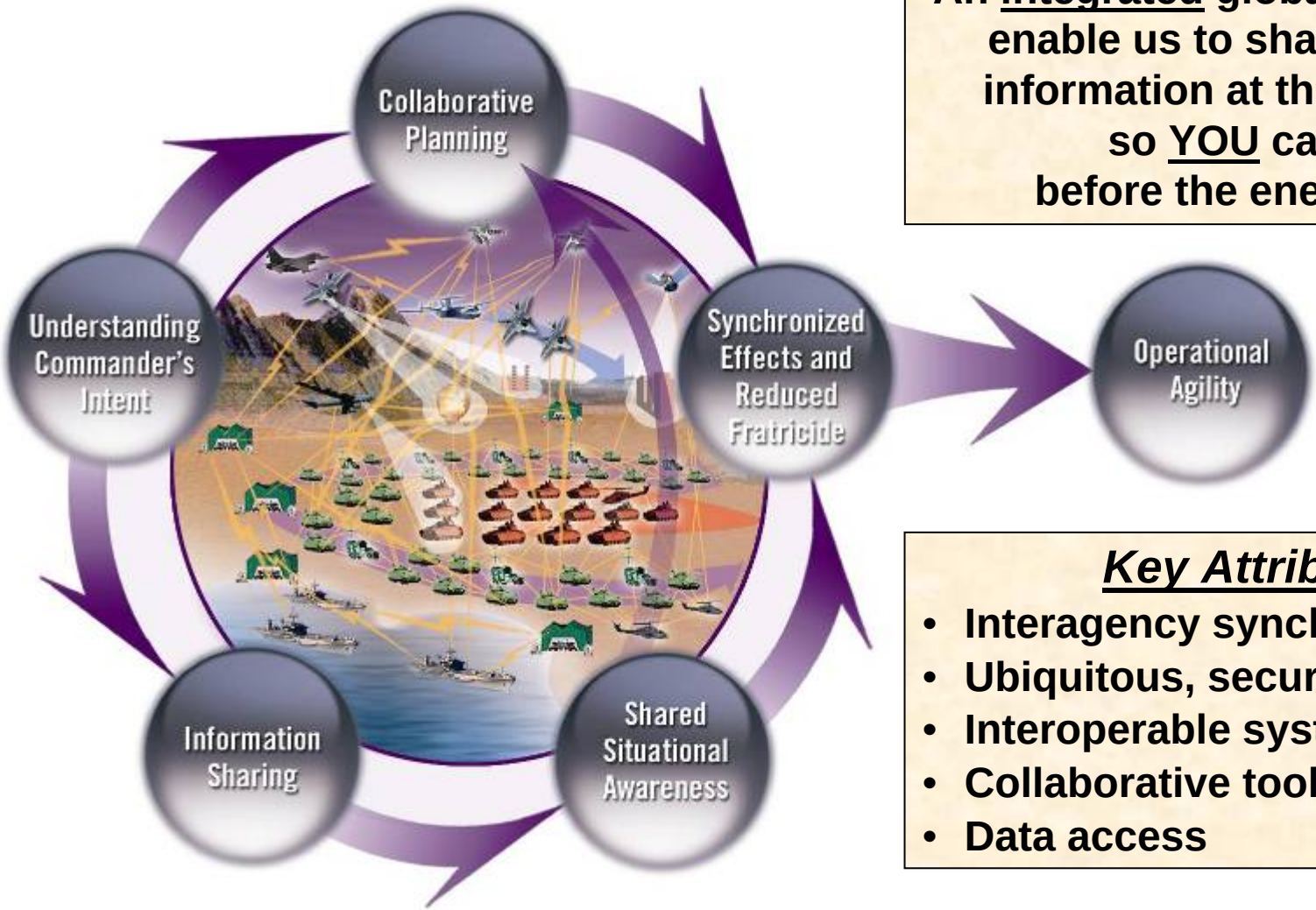


The Foundation for Joint Warfighting

Joint Net-Centric Operations (JNO)

The ability to exploit all human and technical elements of the joint force and its mission partners by fully integrating collected information, awareness, knowledge, experience, and decision making, enabled by secure access and distribution, to achieve a high level of agility and effectiveness in a dispersed, decentralized, dynamic and/or uncertain operational environment. (Derived from Net-Centric Environment JFC)

Joint Net-Centric Operations (JNO)



Vision

An integrated global network will enable us to share the right information at the right time so YOU can act before the enemy acts.

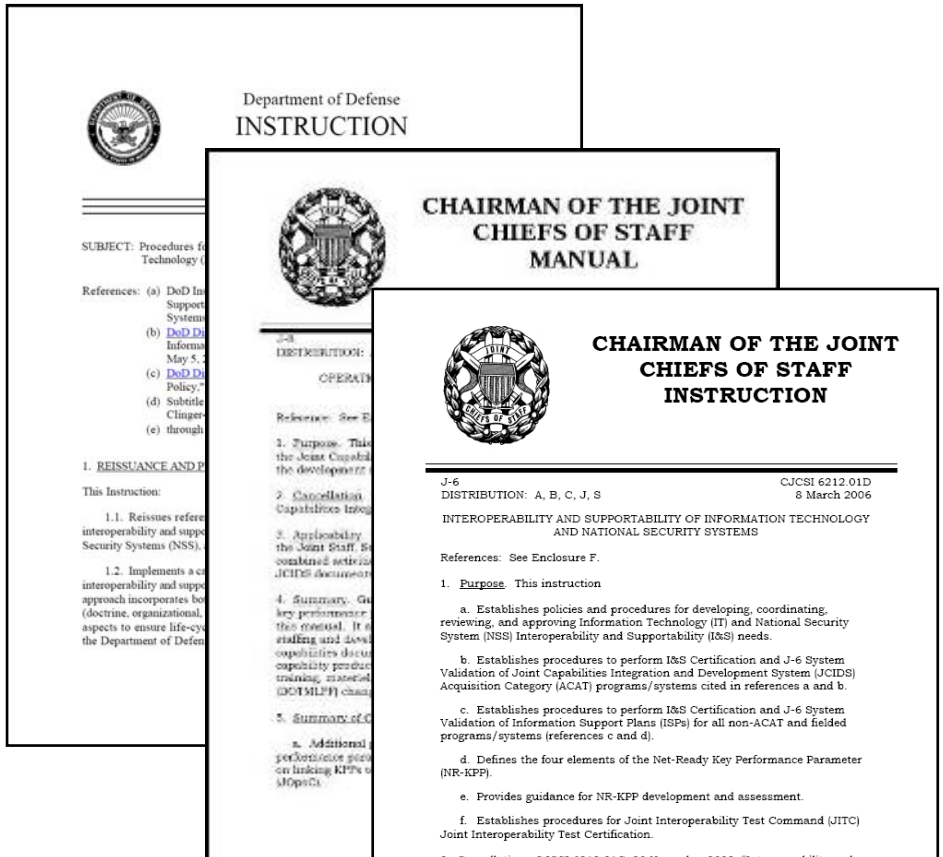
Key Attributes

- **Interagency synchronization**
- **Ubiquitous, secure networks**
- **Interoperable systems**
- **Collaborative tools**
- **Data access**

NR-KPP Requirement

Interoperability Required by:

- Mission Accomplishment
- Law
- DOD 4630 Series
- CJCSIs 3170 and 6212



Department of Defense
INSTRUCTION

CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6212.01D
DISTRIBUTION: A, B, C, J, S 8 March 2006

INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

References: See Enclosure F.

1. Purpose. This instruction

a. Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs.

b. Establishes procedures to perform I&S Certification and J-6 System Validation of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems cited in references a and b.

c. Establishes procedures to perform I&S Certification and J-6 System Validation of Information Support Plans (ISPs) for all non-ACAT and fielded programs/systems (references c and d).

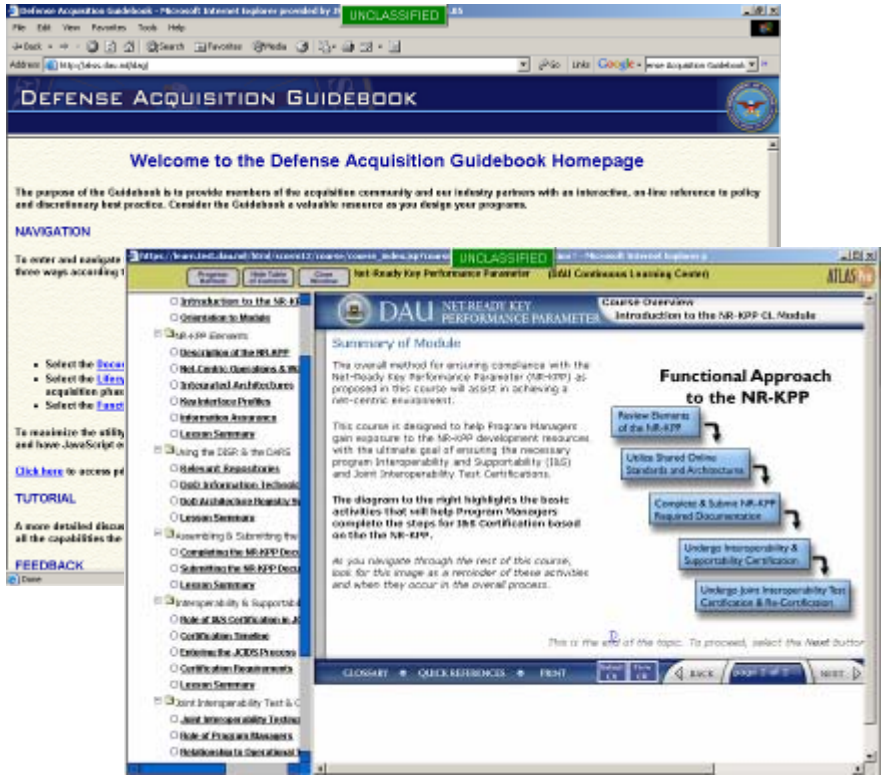
d. Defines the four elements of the Net-Ready Key Performance Parameter (NR-KPP).

e. Provides guidance for NR-KPP development and assessment.

f. Establishes procedures for Joint Interoperability Test Command (JITC) Joint Interoperability Test Certification.

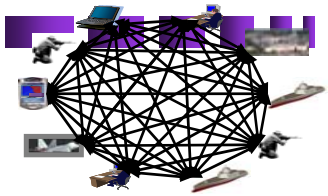
Program Assistance:

- Refined CJCSI 6212.01 (March 2006)
- Program Assistance Visits (Daily)
- NR-KPP DAU Module (May 2006)



http://www.dau.mil

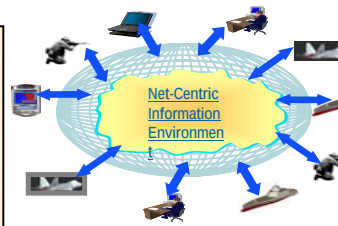
CJCSI 6212.01



May 2000 Focused on one-to-one relationships (point-to-point).

Interoperability KPP (6212.01B)	Threshold	Objective
All top-level Information Exchange Requirements **(IERs)** will be satisfied to the standards specified in the Threshold and Objective values (In blocks when applicable).	**100%** of top-level **IERs** designated critical	**100%** of top-level **IERs**

Nov 2003 Focus shifted to interfaces, net-centric services, data sharing, availability, assurance and correctness – net-readiness and the Net Ready Key Performance Parameter (NR-KPP)

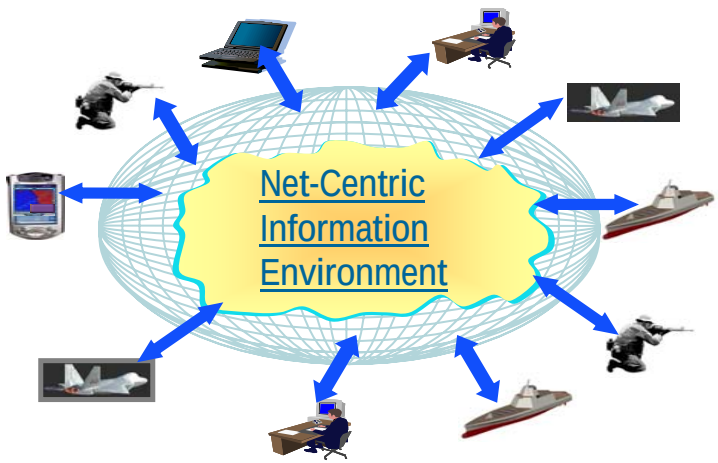


Net-Ready KPP (6212.01C)	Threshold	Objective
All activity interfaces, services, policy-enforcement controls, and data-sharing of the **NCOW-RM** and **GIG-KIPs** will be satisfied.	**100% of** Interfaces Services Policy-enforcement controls Data correctness	**100% of** Interfaces Services Policy-enforcement controls Data correctness

CJCSI 6212.01D NR-KPP (Mar 2006)

Focus on operationalizing & aligning with NR-KPP elements improving understandability and testability.

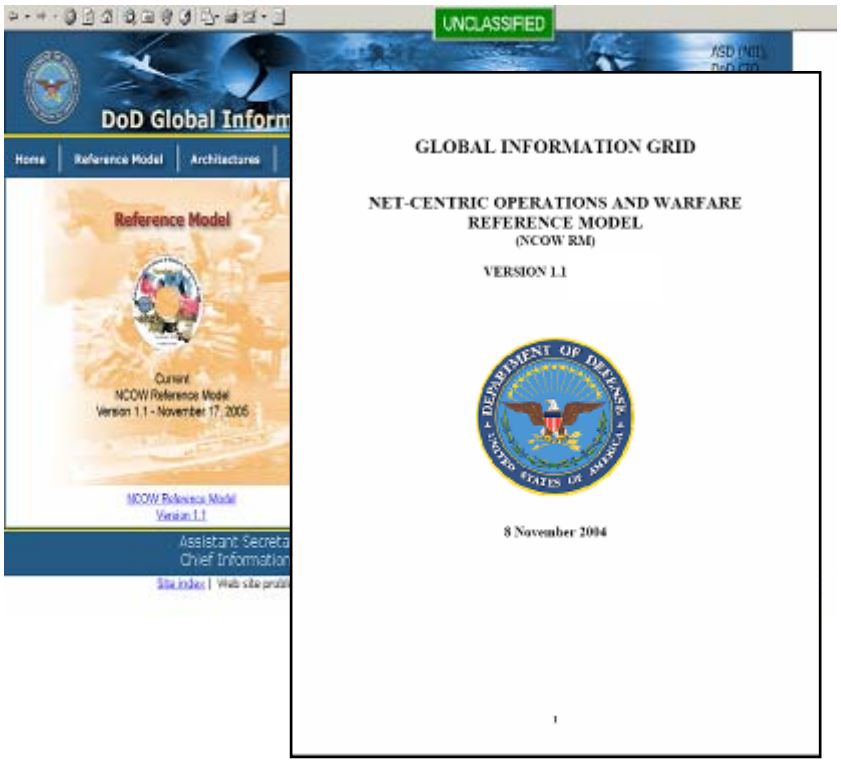
Net-Ready KPP	Threshold	Objective
Net-Ready: The system must support Net-Centric military operations.	Must support execution of **joint critical operational activities** Must satisfy technical requirements of the **NR-KPP elements**.	Must support execution of **all joint critical operational activities** Must satisfy technical requirements of the **NR-KPP elements.**



Net-Centric Operations and Warfare Reference Model

Net-Centricity Enabler:

•Net-Centric Operations and Warfare Reference Model (NR-KPP) – How to Build Guide (Building Code)

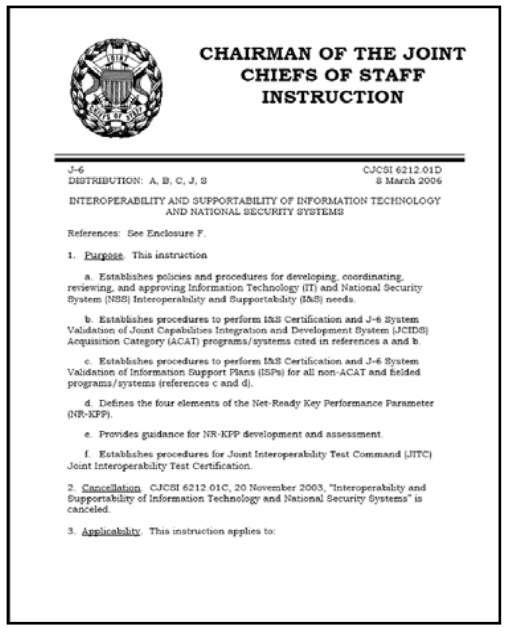


Program Assistance:

•NCOW Reference Model Update (Nov 2005)

•Included Net-Centric Data Strategy in CJCSI 6212.01D (May 2006)

•Drafting CJCSI on Communities of Interest (COI) Governance



CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
INSTRUCTION

J-6 CJCSI 6212.01D
DISTRIBUTION: A, B, C, J, S 8 March 2006

INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

References: See Enclosure F.

1. Purpose. This instruction

a. Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs.

b. Establishes procedures to perform I&S Certification and J-6 System Validation of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems cited in references a and b.

c. Establishes procedures to perform I&S Certification and J-6 System Validation of Information Support Plans (ISPs) for all non-ACAT and fielded programs/systems (references c and d).

d. Defines the four elements of the Net-Ready Key Performance Parameter (NR-KPP).

e. Provides guidance for NR-KPP development and assessment.

f. Establishes procedures for Joint Interoperability Test Command (JITC) Joint Interoperability Test Certification.

2. Cancellation. CJCSI 6212.01C, 20 November 2003, "Interoperability and Supportability of Information Technology and National Security Systems" is canceled.

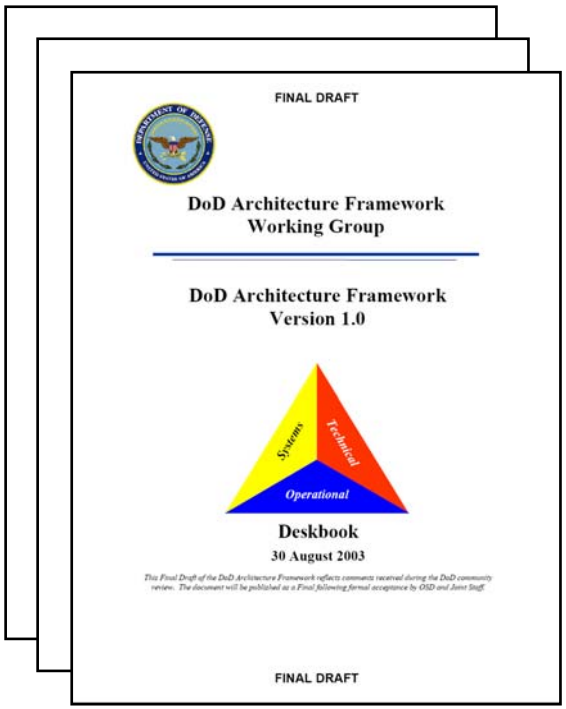
3. Applicability. This instruction applies to:

Architectures

Net-Centricity Enabler:

•Architecture Development

•Documents Capabilities and Interoperability Requirements


FINAL DRAFT

DoD Architecture Framework Working Group

DoD Architecture Framework Version 1.0

Systems
Technical
Operational

Deskbook

30 August 2003

This Final Draft of the DoD Architecture Framework reflects comments received during the DoD community review. The document will be published as a Final following formal acceptance by OSD and Joint Staff

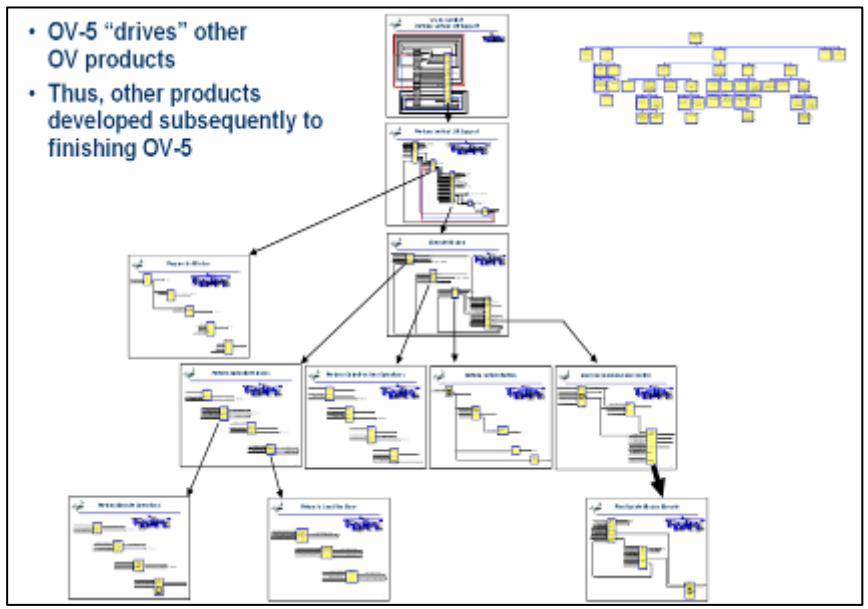
FINAL DRAFT

Program Assistance:

•DOD Architecture Framework (DODAF)

•DODAF Working Group for Version 2.0

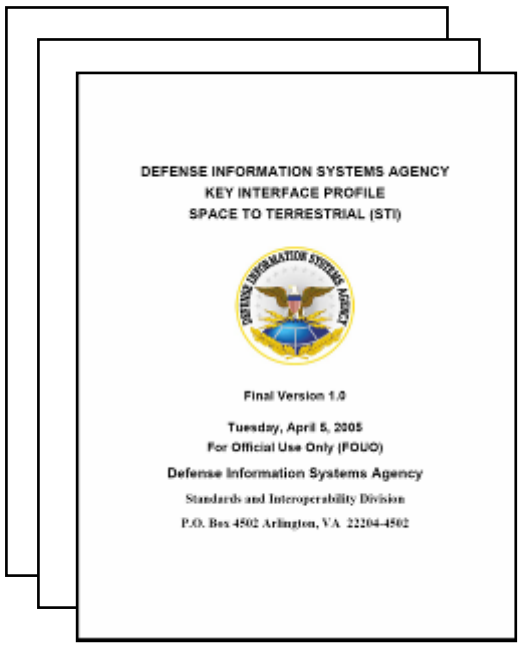
•Developing JCA based Warfighting Mission Area Enterprise Architecture



Key Interface Profiles

Net-Centricity Enabler:
- Key Interface Profiles (KIPs)
- Drives Programs to Standardized Approach to Interoperability

Program Assistance:
- Activated KIP Website (Nov 2005)
- Completed Transport Family (Mar 2006)

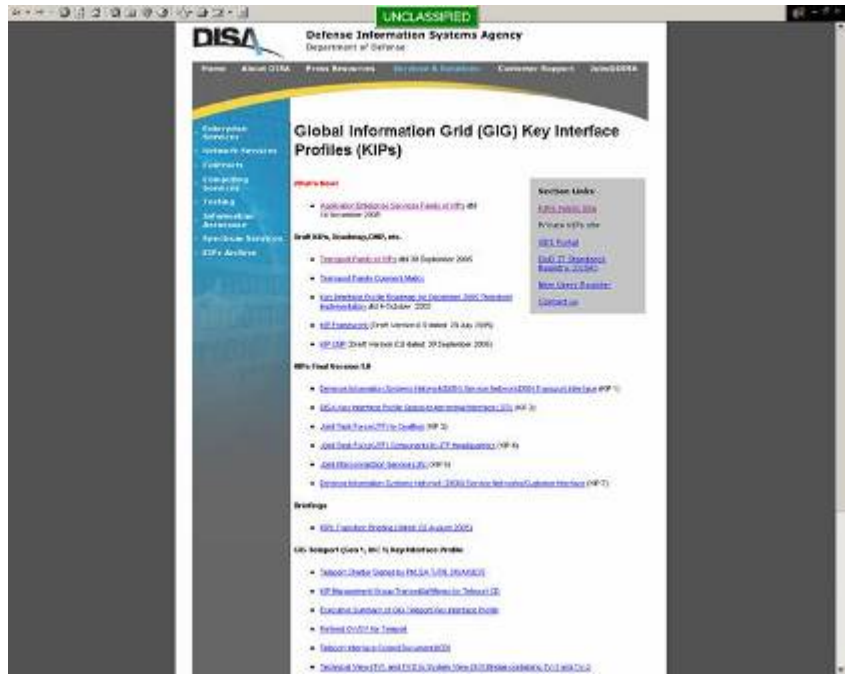


DEFENSE INFORMATION SYSTEMS AGENCY
KEY INTERFACE PROFILE
SPACE TO TERRESTRIAL (STI)

Final Version 1.0

Tuesday, April 5, 2005
For Official Use Only (FOUO)

Defense Information Systems Agency
Standards and Interoperability Division
P.O. Box 4502 Arlington, VA 22204-4502



https://kips.disa.mil

Information Technology Standards

Net-Centricity Enabler:

•DOD Information Technology Standards Registry (DISRonline)

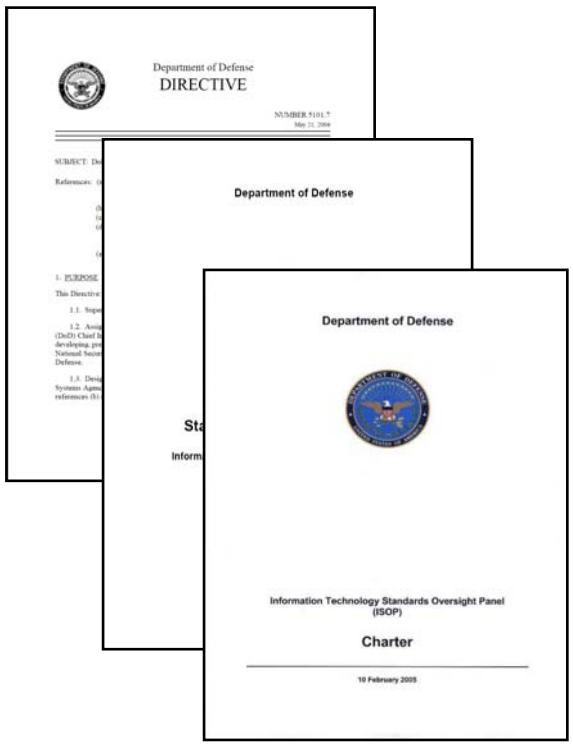
•Forces Programs to Common Technology Solutions (Code)

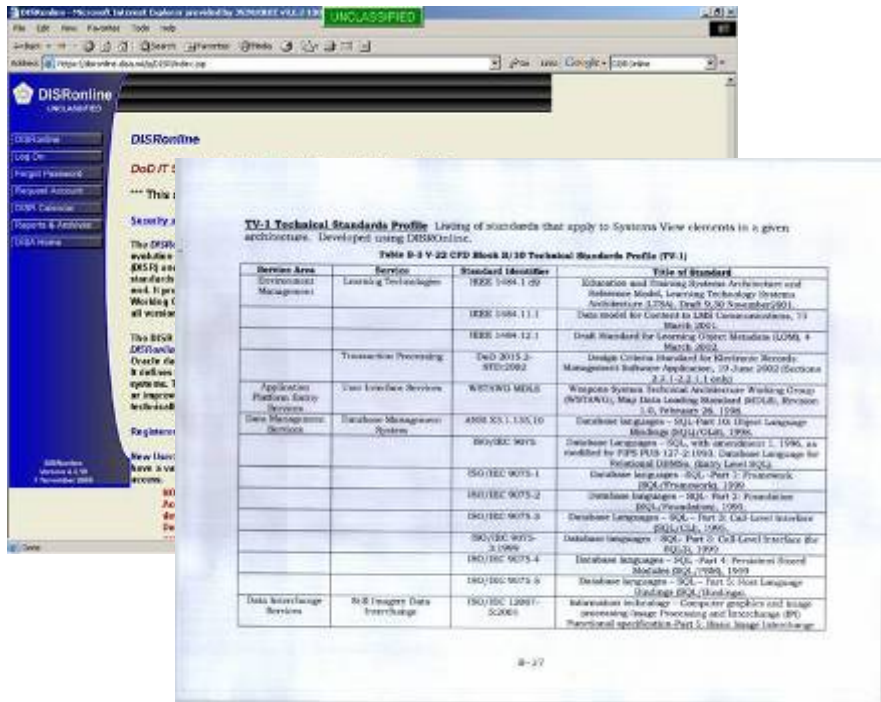
•DOD Technical Standards

Program Assistance:

•One Official Technical Standards Authoritative Source

•Automated Development Tools to Develop the Technical View Architecture Product





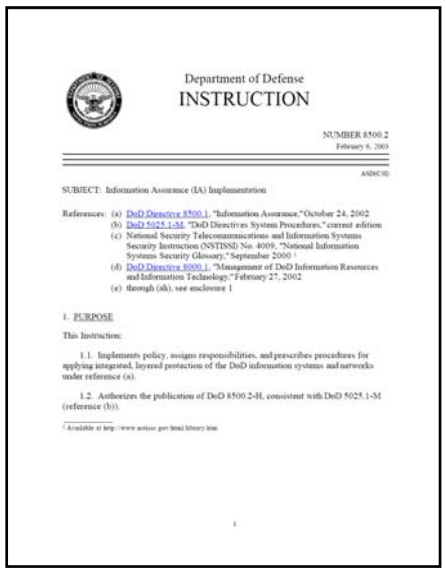
Information Assurance

Net-Centricity Enabler:

•Force Early Compliance Strategy of Information Assurance Requirements

Program Assistance:

•Refined guidance in CJCSI 6212.01D (Mar 2006)



Department of Defense
INSTRUCTION

NUMBER 8500.2
February 6, 2003

ASD(C3I)

SUBJECT: Information Assurance (IA) Implementation

References: (a) DoD Directive 8500.1, "Information Assurance," October 24, 2002
(b) DoD 5025.1-M, "DoD Directives System Procedures," current edition
(c) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," September 2000 [1]
(d) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002
(e) through (ah), see enclosure 1

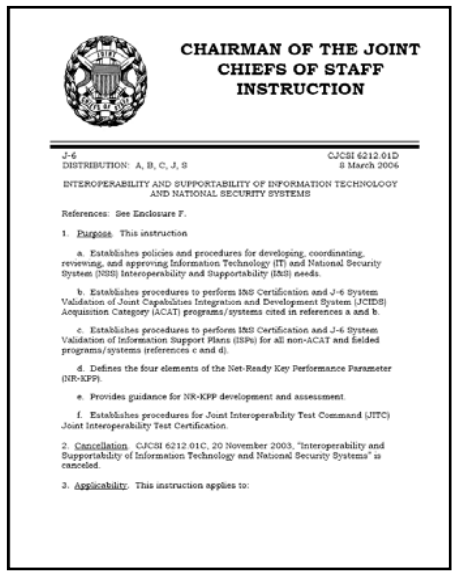
1. PURPOSE

This Instruction:

1.1. Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under reference (a).

1.2. Authorizes the publication of DoD 8500.2-H, consistent with DoD 5025.1-M (reference (b)).

[1] Available at http://www.nstissc.gov/html/library.html



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, J, S

CJCSI 6212.01D
8 March 2006

INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

References: See Enclosure F.

1. Purpose. This instruction

a. Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs.

b. Establishes procedures to perform I&S Certification and J-6 System Validation of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems cited in references a and b.

c. Establishes procedures to perform I&S Certification and J-6 System Validation of Information Support Plans (ISPs) for all non-ACAT and fielded programs/systems (references c and d).

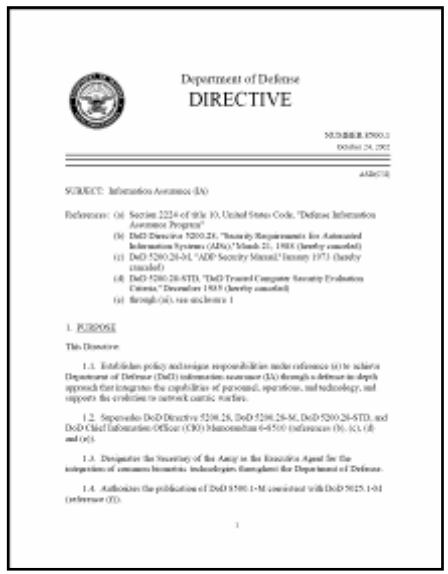
d. Defines the four elements of the Net-Ready Key Performance Parameter (NR-KPP).

e. Provides guidance for NR-KPP development and assessment.

f. Establishes procedures for Joint Interoperability Test Command (JITC) Joint Interoperability Test Certification.

2. Cancellation. CJCSI 6212.01C, 20 November 2003, "Interoperability and Supportability of Information Technology and National Security Systems" is canceled.

3. Applicability. This instruction applies to:



Department of Defense
DIRECTIVE

NUMBER 8500.1
October 24, 2002

ASD(C3I)

SUBJECT: Information Assurance (IA)

References: (a) Section 2224 of title 10, United States Code, "Defense Information Assurance Program"
(b) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988 (hereby canceled)
(c) DoD 5200.28-M, "ADP Security Manual," January 1973 (hereby canceled)
(d) DoD 5200.28-STD, "DoD Trusted Computer Security Evaluation Criteria," December 1985 (hereby canceled)
(e) through (ai), see enclosure 1

1. PURPOSE

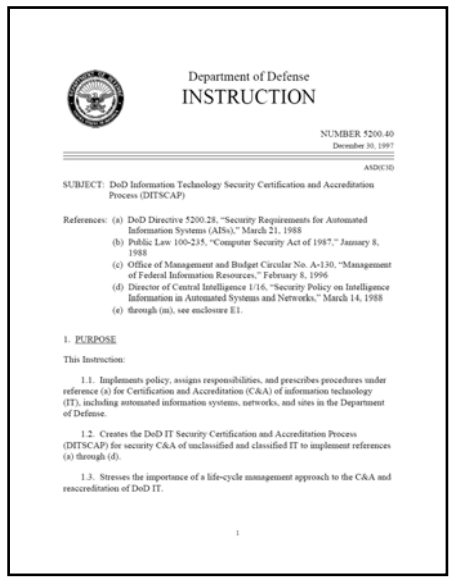
This Directive:

1.1. Establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

1.2. Supersedes DoD Directive 5200.28, DoD 5200.28-M, DoD 5200.28-STD, and DoD Chief Information Officer (CIO) Memorandum 6-8510 (references (b), (c), (d) and (e)).

1.3. Designates the Secretary of the Army as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

1.4. Authorizes the publication of DoD 8500.1-M consistent with DoD 5025.1-M (reference (f)).



Department of Defense
INSTRUCTION

NUMBER 5200.40
December 30, 1997

ASD(C3I)

SUBJECT: DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

References: (a) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988
(b) Public Law 100-235, "Computer Security Act of 1987," January 8, 1988
(c) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1996
(d) Director of Central Intelligence 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks," March 14, 1988
(e) through (m), see enclosure E1.

1. PURPOSE

This Instruction:

1.1. Implements policy, assigns responsibilities, and prescribes procedures under reference (a) for Certification and Accreditation (C&A) of information technology (IT), including automated information systems, networks, and sites in the Department of Defense.

1.2. Creates the DoD IT Security Certification and Accreditation Process (DITSCAP) for security C&A of unclassified and classified IT to implement references (a) through (d).

1.3. Stresses the importance of a life-cycle management approach to the C&A and reaccreditation of DoD IT.

NR-KPP Testing

Net-Centricity Enabler:

•Validates and Ensures Interoperability

•Verifies Net-Centric Approach to Information Sharing

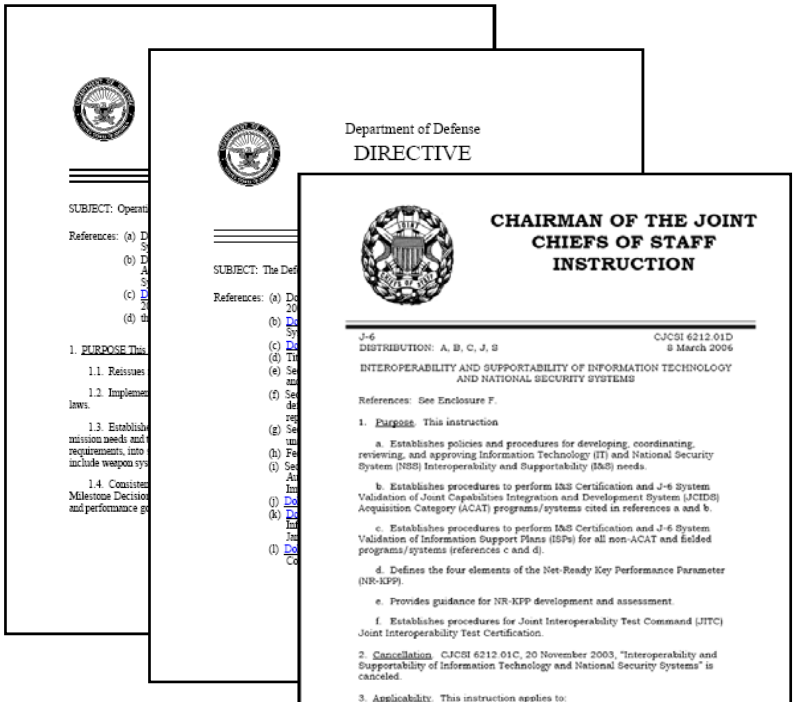
Program Assistance:

•Rewrote CJCSI 6212.01D Test Enclosure

•JITC Test and Evaluation Master Plan (TEMP) Development Assistance

•NR-KPP OT Guide (Sep 2005)

•Testing Chapter in NR-KPP Module (May 2006)



Department of Defense
DIRECTIVE

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6212.01D
DISTRIBUTION: A, B, C, J, S 8 March 2006

INTEROPERABILITY AND SUPPORTABILITY OF INFORMATION TECHNOLOGY AND NATIONAL SECURITY SYSTEMS

References: See Enclosure F.

1. Purpose. This instruction

a. Establishes policies and procedures for developing, coordinating, reviewing, and approving Information Technology (IT) and National Security System (NSS) Interoperability and Supportability (I&S) needs.

b. Establishes procedures to perform I&S Certification and J-6 System Validation of Joint Capabilities Integration and Development System (JCIDS) Acquisition Category (ACAT) programs/systems cited in references a and b.

c. Establishes procedures to perform I&S Certification and J-6 System Validation of Information Support Plans (ISPs) for all non-ACAT and fielded programs/systems (references c and d).

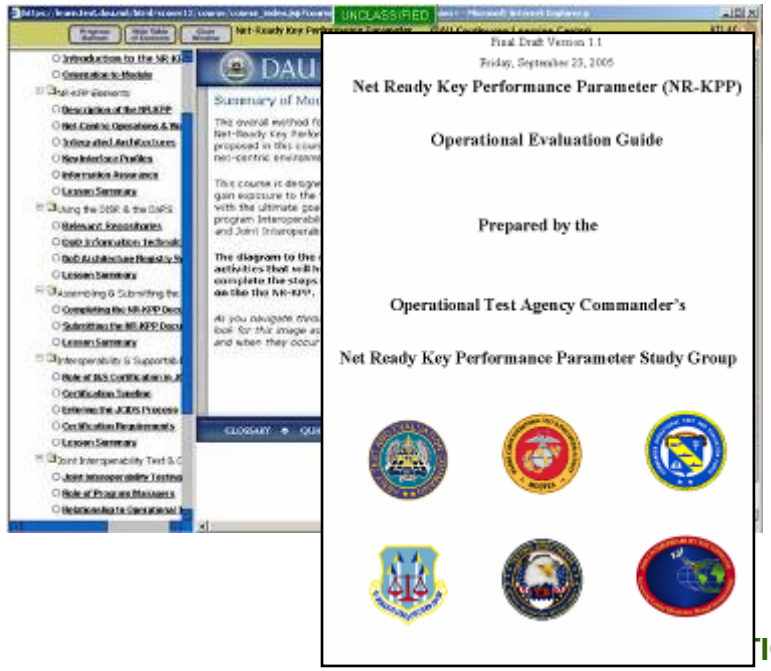
d. Defines the four elements of the Net-Ready Key Performance Parameter (NR-KPP).

e. Provides guidance for NR-KPP development and assessment.

f. Establishes procedures for Joint Interoperability Test Command (JITC) Joint Interoperability Test Certification.

2. Cancellation. CJCSI 6212.01C, 20 November 2003, "Interoperability and Supportability of Information Technology and National Security Systems" is canceled.

3. Applicability. This instruction applies to:



UNCLASSIFIED

Final Draft Version 1.1
Friday, September 23, 2005

Net Ready Key Performance Parameter (NR-KPP)

Operational Evaluation Guide

Prepared by the

Operational Test Agency Commander's

Net Ready Key Performance Parameter Study Group

Conclusion