CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

Directive current as of 28 September 2010

J6 CJCSI 8010.01B
DISTRIBUTION: A, B, C, J, S 8 September 2006

JOINT COMMUNITY WARFIGHTER CHIEF INFORMATION OFFICER

Reference: See Enclosure A.

1. Purpose. This instruction assigns the position of Joint Community Warfighter (JCW) Chief Information Officer (CIO), establishes applicable policy, and outlines the duties and responsibilities of that position.

2. Cancellation. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 8010.01A, 13 June 2003, "Joint Community Chief Information Officer," is canceled.

3. Applicability. This instruction applies to the Joint Staff, combatant commands, and joint activities that coordinate through the Chairman of the Joint Chiefs of Staff. With regards to Capital Planning and Investment Control, the JCW CIO will represent the JCW in acquisition category (ACAT) and non-ACAT programs affecting the joint warfighting (deployable and non-deployable) aspects of the Global Information Grid (GIG). Consistent with 10 USC 2223, the Joint Staff/J-6 will act on behalf of the Joint Staff in ensuring interoperability among DOD components.

4. Policy

a. The Director, Command, Control, Communications, and Computer Systems Directorate (J-6), Joint Staff, is designated the JCW CIO, acting on behalf of the Chairman of the Joint Chiefs of Staff as prescribed in references DODD 8000.1 and DODD 8100.1.

b. Vice Director, Joint Staff, retains the responsibilities of the Joint Staff CIO. Details of these responsibilities are found in reference a.

c. Director for Intelligence (J-2), Joint Staff, will represent the JCW at the

Intelligence Community (IC) CIO Executive Council for intelligence and intelligence-related national security systems (NSS).

d. Director of Operations (J-3), Joint Staff, will guide C4 requirements and attendant architectural products through the clear delineation of global and regional operational requirements.

e. Combatant commanders will designate a CIO and develop appropriate guidance for their area of responsibility (see reference b). The combatant command CIOs shall use the JCW CIO as their conduit to the DOD CIO and Executive Board. With the concurrence of the Chairman of the Joint Chiefs of Staff and the cognizant combatant commander, CIOs of the combatant commands may directly contact the DOD CIO, when required in unusual circumstances, and should keep the JCW CIO informed. It is recognized that USJFCOM and USSTRATCOM are members of the DOD CIO Executive Board and have the latitude to directly contact the DOD CIO when desired. Combatant command CIOs may use the J-2 as the conduit for issues of intelligence and intelligence-related NSS to the IC CIO Executive Council and should keep the JCW CIO informed.

f. By virtue of their respective transformational roles as dictated by the Unified Command Plan, USSTRATCOM, USJFCOM, and USSOCOM will advocate the following information technology (IT) themes and issues:

(1) Command, control protection and availability of the GIG. (USSTRATCOM)

(2) Interoperability of major components of the GIG. (USJFCOM)

(3) Implementation of GIG transformational capabilities to support the War on Terrorism. (USSOCOM)

g. Joint Staff directorates will use the JCW CIO as a conduit to the DOD CIO Executive Board or J-2 for access to the IC CIO Executive Council on issues that involve their functional area and affect the JC. J-2 will coordinate with J-6 as JCW CIO on intelligence systems that impact or interact with operational systems.

h. By promulgating and enforcing interoperability standards and applying IT linkage to operational requirements, the JCW CIO and combatant commander CIOs will assist the DOD CIO in fulfilling the DOD CIO mandated responsibilities.

5. Definitions. Refer to the Glossary.

6. Responsibilities of the JCW CIO.

a. **Joint IT, including NSS, Strategic Planning**: Develop an IT planning, prioritization, and synchronization mechanism (Joint C4 Campaign Plan) to ensure alignment with the combatant commander's warfighting priorities.

b. **IT Governance and Capital Planning and Investment Control**

(1) Advocate the development and priority of joint IT as the warfighting mission area (WMA) lead. Represent the IT requirements of combatant commands and translate priorities into actionable programmatic consideration for the JROC and DOD CIO.

(2) Per reference b, designate joint automated information systems, advocating the termination of duplicative systems via established joint requirements and oversight mechanisms.

(3) Advise and assist combatant command CIOs on policy and capital investment issues pertaining to IT and NSS.

(4) Per reference d, capture and synchronize emerging observations and lessons learned into greater IT standardization process.

(5) Establish an overarching JCW CIO Council responsible for collaboration, management, and integration of cross-cutting issues, including IT architectures, interoperability, information management, information resource management (IRM), information dissemination management, enterprise global data management, and strategic plans. Membership is comprised of representatives from the agencies, combatant commands, and the Joint Staff directorates.

c. **Net-Centric Data Strategy Implementation**. In accordance with references r and s, in coordination with the ASD(NII)/DOD CIO; Commander, USJFCOM; and the other DOD components as needed, establish policy and procedures to ensure that domains within the WMA promote net-centric data sharing; and effectively enable COIs, including adjudicating conflicts in metadata agreements and identifying authoritative sources.

d. **Enterprise Architecture Development and IT Standards**

(1) In accordance with reference e, ensure, with the Joint Staff/J-3, USD(AT&L), the ASD(NII)/DOD CIO, the Director of Operational Test and Evaluation (DOT&E), CDRUSJFCOM, and the DOD components, that insights gained from combined, joint, and coalition exercises, demonstrations, experiments, and operations are included in JCIDS analysis to facilitate improvements in IT and NSS interoperability and supportability.

(2) In accordance with reference f, provide the DOD CIO the joint military priorities for development and selection of IT standards conformance issues.

(3) In accordance with reference c, lead the development of the Joint Operational Architecture describing key information elements, information flow, and information exchanges in support of combined and/or joint task force operations across all relevant mission areas.

(4) In accordance with reference e, establish policy and procedures, with the CDRUSJFCOM, CDRUSSOCOM, and the other DOD components, for the development, coordination, review, and approval of IT and NSS interoperability and supportability needs.

(a) Direct the use of integrated architectures to facilitate the identification of IT and NSS interoperability and supportability needs within a capability focused, effects-based context.

(b) Develop, approve, and issue joint concepts and associated operational procedures to achieve interoperability and supportability of IT and NSS employed by US Military Forces and, where required, with joint, combined, and coalition forces and with other US government departments and agencies.

(c) Review, certify, and validate sufficiency of the net readiness-key performance parameters.

(d) Maintain, with the USD(AT&L), the ASD(NII)/DODCIO, the DOT&E, and the CDRUSJFCOM, procedures for verification and certification of interoperability based on meeting the requirements of the NR-KPP for new and fielded IT and NSS throughout a system's life.

(e) Through the JROC and DOD CIO, determine compliance of interoperability standards by reviewing the interoperability key performance parameters of capabilities documents required by CJCSI 3170.01E and 6212.01.D. In accordance with reference l, guide Service architectural development with singular operational and/or technical view of joint military priorities.

e. **Information Assurance and IA Workforce**

(1) In accordance with reference g, integrate IA readiness in CJCS readiness system.

(2) Per reference h, ensure WMA policies are incorporated into the National Defense University curriculum. Assist the DOD CIO in the

development and implementation of sound information assurance policies and guidance.

f. **Network Operations**. In accordance with reference i, lead development of common network operations tasks for inclusion into the Universal Joint Task List and promulgate associated TTPs within the combatant commands.

(1) Lead the development of a framework for a theater network common operational picture.

(2) In coordination with CDRUSSTRATCOM, review joint C4 requirements for inclusion of network management and surveillance elements.

7. Summary of Changes. Revised responsibilities of the joint community CIO. Recognized USSTRATCOM CIO as DOD CIO Executive Board member. J-6 will guide development of Service architectures with an integrated operational and/or technical view architecture. Deleted enclosure that summarized the responsibilities for the DOD and Service CIO as not applicable to this instruction. Updated contents of references (Enclosure A).

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page-http://www.dtic.mil/cjcs_directives. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Enclosures:

A – References
GL - Glossary

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)	4
Director, National Intelligence	2
Director, National Security Agency	2
Director, Defense Information Systems Agency	2
Director, General Services Administration	2

(INTENTIONALLY BLANK)

ENCLOSURE A

REFERENCES

a. JSI 8000.01 Series, "Joint Staff Chief Information Officer"

b. DOD Directive 8000.1, 27 February 2002, "Management of DOD Information Resources and Information Technology"

c. DOD Directive 8100.1, 19 September 2002, "Global Information Grid (GIG) Overarching Policy"

d. CJCSI 3150.25 Series, "Joint Lessons Learned Program"

e. DOD Directive 4630.5, 5 May 2004, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)"

f. DOD Directive 5101.7, 21 May 2004, "DOD Executive Agent for Information Technology Standards"

g. DOD Instruction 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"

h. DOD Directive 8115.01, 10 October 2005, "Information Technology Portfolio Management"

i. G&PM 10-8460, 24 August 2000, "Department of Defense (DOD) Chief Information Officer (CIO) Guidance and Policy Memorandum No. 10-8460-Network Operations"

j. 40 USC Chapter 25, Sections 1401-1503 (aka Clinger-Cohen Act of 1996 and Information Technology Management Reform Act (ITMRA))

k. 44 USC Chapter 35, Sections 3501-3520 (Paperwork Reduction Act of 1995)

l. 10 USC Chapter 131, Section 2223 (aka Strom Thurmond Act)

m. Executive Order 13011, Federal Information Technology

n. Office of Management and Budget Circular A-130, 28 November 2000, "Management of Federal Information Resources"

o. Government Performance and Results Act (GPRA) of 1993, (Public Law 103-62)

p. CJCSI 3170.01 Series, "Joint Capabilities Integration and Development System"

q. CJCSI 6212.01 Series, "Interoperability and Supportability of Information Technology Systems and National Security Systems"

r. DOD Information Management (IM) Strategic Plan, 19 October 1999

s. Director of Central Intelligence (DCI) Directive 1/6, 4 February 2000, "Intelligence Community Chief Information Officer, Intelligence Community Chief Information Officer Executive Council, Intelligence Community Chief Information Officer Working Council"

t. CJCSI 5123.01 Series, "Charter of the Joint Requirements Oversight Council"

u. DOD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 11-8450, 6 April 2001, "Global Information Grid (GIG) Computing"

v. Deputy Secretary of Defense memorandum 14234-04, 13 April 2005, "DOD Chief Information Officer Executive Board Charter"

w. DODD 5144.1, 2 May 2005, "Assistant Secretary of Defense for Networks and Information Integration/DOD Chief Information Officer (ASD(NII)/DOD CIO)"

x. DODD 8320.2, 2 December 2004, "Data Sharing in a Net-Centric Department of Defense"

y. Department of Defense Chief Information Officer memorandum, 9 May 2003, "DoD Net-Centric Data Strategy"

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

ACAT	acquisition category
C4	command, control, communications, and computers
C-CA	Clinger-Cohen Act of 1996
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
DOD	Department of Defense
DOT&E	Director of Operational Test and Evaluation
GIG	Global Information Grid
IC	Intelligence Community
IM	information management
IRM	information resource management
IS	information system
IT	information technology
ITCIP	Information Technology Capital Investment Portfolio
J-2	intelligence directorate of a joint staff
J-6	command, control, communications, and computer systems directorate of a joint staff
JC	Joint Community
JCW	Joint Community Warfighter
JROC	Joint Requirements Oversight Council
NSS	national security systems
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
USSOCOM	United States Special Operations Command
WMA	warfighting mission area

PART II--DEFINITIONS

combatant command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities.

Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes national security systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

information assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DODD S-3600.1)

information management. The planning, budgeting, collecting, collating, correlating, manipulating, fusing, storing, archiving, retrieving, controlling, disseminating, protecting, and destroying of information throughout its life cycle.

information resource management. The process of managing information resources to accomplish agency missions and to improve agency performance. The term encompasses both information and the related resources such as personnel, equipment, funds, and information technology.

information system. (1) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 USC 3502(8)). (2) The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. In addition, the hardware, software, and personnel associated with a system or system-of-systems that processes information to accomplish a function. (DCI Directive 1/6)

information technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a component directly or used by a contractor under a contract with the component that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term does not include any equipment that is acquired by a federal contractor incidental to a federal contract.

Information Technology Capital Investment Portfolio (ITCIP). An investment governance mechanism that supports the Department of Defense implementation of the Clinger-Cohen Act of 1996, Division E, and other laws, policies, and guidance for managing information technology (IT) investments. The ITCIP is intended to provide the Chief Information Officer with better information to support management and investment decisions; to assist functional managers to effectively build and manage IT portfolios to fulfill strategic visions, goals, and related measures of performance; and to assist program managers to effectively manage performance, cost, and schedule risks in the acquisition of IT.

Joint Community. The directorates on the Joint Staff, combatant commands, and joint activities that are responsible to the Chairman of the Joint Chiefs of Staff.

Joint Requirements Oversight Council (JROC). Senior advisory council to the Chairman of the Joint Chiefs of Staff that assists in identifying and assessing the priority of joint military requirements, assessing warfighting capabilities, evaluating alternatives to any acquisition program, assigning priority among existing and future major programs, reviewing major warfighting deficiencies that require major acquisition programs, and resolving cross-Service requirement issues.

national security systems. Any telecommunications or information system operated by the U.S. government, the function, operation, or use of (1) involves intelligence activities, (2) involves cryptologic activities related to national security, (3) involves command and control of military forces, (4) involves equipment that is an integral part of a weapon or weapons system, or (5) is critical to the direct fulfillment of military or intelligence missions. They do not include systems that are to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).