



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C

CJCSI 8010.01C
1 November 2013


JOINT COMMUNITY WARFIGHTER CHIEF INFORMATION OFFICER

Reference: See Enclosure B.

1. Purpose. This instruction assigns the position of Joint Community Warfighter Chief Information Officer (JCW CIO), establishes applicable policy, and outlines the duties and responsibilities of that position as directed by reference a. Further, this addresses policies and procedures for Warfighting Mission Area (WMA) Information Technology (IT) Portfolio Management.
2. Cancellation. CJCSI 8010.01B, 8 September 2006 (Current as of 28 September 2010), "Joint Community Warfighter Chief Information Officer" and CJCSI 8410.01A, 20 March 2009, (Current as of 11 May 2011), "Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing" are canceled.
3. Applicability. This instruction applies to the Joint Staff, Combatant Commands, Military Departments, Services, Defense Agencies, and joint and combined activities that coordinate through the Chairman of the Joint Chiefs of Staff.
4. Definitions. See Glossary.
5. Releasability. This instruction is approved for public release; distribution is unlimited. DoD Components, other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page-Electronic Library at: <http://www.dtic.mil/cjcs_directives>.

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

For the Chairman of the Joint Chiefs of Staff:


DAVID L. GOLDFEIN, Lt Gen, USAF
Director, Joint Staff

Enclosures:

- A – Joint Community Warfighter Chief Information Officer
- B – References
- GL - Glossary

ENCLOSURE A

JOINT COMMUNITY WARFIGHTER CHIEF INFORMATION OFFICER

1. Overview

a. The Joint Staff Director for Command, Control, Communications, and Computers/Cyber (J-6) serves as the Joint Staff Chief Information Officer (JS CIO) and is also designated as the Joint Community Warfighter Chief Information Officer (JCW CIO). As the JCW CIO, the J-6 will:

(1) Ensure that the Component complies with, and promptly, efficiently, and effectively implements the policies and responsibilities in reference a, and the requirements of Titles 44, 40, 10 (Sections 2223 and 2224) and OMB Circular A-130.

(2) Advocate for the joint community in acquisition category (ACAT) and non-ACAT programs affecting the deployable and non-deployable aspects of the Department of Defense Information Network (DoDIN), also known as the Global Information Grid (GIG). Consistent with reference c, the JCW CIO will act on behalf of the Joint Staff in ensuring interoperability among DoD Components, who are primary owners of Warfighter Mission Area (WMA) capabilities.

b. Further, the WMA objective is to enable joint military operational effectiveness through information services to the warfighter. WMA provides the framework to manage warfighter Information Technology (IT) investments as portfolios focusing on improving joint capabilities and mission outcomes, and enhancing the Chairman of the Joint Chiefs of Staff's joint warfighting priorities.

c. Responsibilities of JS J-6 include all functions previously consolidated under JS J-8 as the Deputy Director for Command, Control, Communications and Computers (DDC4) and are transferred to Director, J-6 to include Chair of the Military Communications-Electronics Board (MCEB), reference s; Joint Staff CIO, reference f; and Director of Joint Staff IT Transformation per reference d.

2. Policy

a. The Joint Staff Director for Command, Control, Communications, and Computers/Cyber (J-6) /Chief Information Officer (JS J-6) is designated the JCW CIO, and WMA lead, acting on behalf of the Chairman of the Joint Chiefs of Staff as prescribed in references a and b. The JCW CIO will advocate and enable joint military operational effectiveness through effective warfighter IT

and interoperability of components with the DoDIN. IAW with reference aa, the JCW CIO is also appointed the WMA Principal Accrediting Authority.

b. The JCW CIO is a member of the DoD CIO Executive Board Charter as prescribed in reference e.

c. The JCW CIO serves as a Tri-chair of the Joint Information Environment (JIE) Executive Committee (EXCOM) along with DoD CIO and USCYBERCOM/J-6 at reference ac.

d. By promulgating and enforcing interoperability standards and applying IT linkage to operational requirements, the JCW CIO and Combatant Command CIOs will assist the DoD CIO in fulfilling the DoD CIO mandated responsibilities at reference e.

3. Responsibilities of the JCW CIO

a. Joint IT, including NSS, Strategic Planning: Develop an IT planning, prioritization, and synchronization mechanism to ensure alignment with the Combatant Commander's warfighting priorities for the WMA.

b. IT Governance and Capital Planning and Investment Control (WMA IT Portfolio Management)

(1) Internal Joint Staff IT Portfolio Management is prescribed by references a, i, and j for Joint Staff IT investments that are in the DoD IT Portfolio Repository (DITPR), the Select and Native Programming Data Input System (SNaP-IT), and the DITPR/SNaP-IT/ investments in the DoD IT Investment Portal (DITIP) and are not covered by this CJCSI.

(2) The JCW CIO J-6 staff provides assistance to cross-capability assessments, e.g., gap assessment, redundancy analysis, capability and mission assessment, research support, JCIDS Net-Ready Key Performance Parameter (NR-KPP) certification, C4 mission thread assessment, data strategy, solution and reference architecture as required by the Functional Capability Boards (FCBs) IAW with references l and m.

(3) FCB portfolio reviews will ensure IT JCIDS investments comply with reference m, ensuring JIE and reference o, Mission Partner Environment (MPE) enablement.

(4) Represent the IT requirements of Combatant Commands and translate priorities into actionable programmatic consideration for the JROC and DoD CIO in accordance with reference p.

- (5) FCBs will monitor and manage the Data Service Environment content to support data requirements within their functional areas in accordance with JROC approved documents.
- (6) Identify information sharing problems within their domains, and inform the appropriate data governance forum to address the issue.
- (7) Designate joint automated information systems, advocating the termination of duplicative systems via cloud-based joint requirements and oversight mechanisms. Per reference q, agencies are required to evaluate safe, secure cloud computing options before making any new IT investments.
- (8) Advise and assist Combatant Command CIOs on policy and capital planning and investment control issues pertaining to IT and NSS per reference a, c, and h. Reference n is to inform Component planning in the DoD budget cycle.
- (9) Capture and synchronize emerging observations and lessons learned into greater IT standardization process per reference r.
- (10) Use the Military Communications-Electronics Board (MCEB) as in reference s as the overall governance forum responsible for collaboration, management, and integration of cross-cutting issues, including IT architectures, interoperability, information management, information resource management, information dissemination management, enterprise global data management, and strategic plans. Membership is comprised of representatives from the Combatant Commands, Services, Agencies and the Joint Staff directorates.
- (11) Facilitate delivery of integrated C4/Cyber capabilities to increase joint operational effectiveness and balance warfighter demands within existing resource constraints.

c. Data-Centric Strategy Implementation

- (1) Coordinate with the DoD CIO and the other DoD Components as needed to establish policy and procedures to ensure that domains within the WMA promote data-centric sharing; and effectively enable Communities of Interests (COIs), including adjudicating conflicts in metadata agreements and identifying authoritative sources in accordance with references b and t.
- (2) Participate in and/or lead management of the information exchange domain in coordination with DoD CIO, the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), and other key stakeholders in accordance with reference u.

(3) Coordinate and facilitate Combatant Commands, Services, Agencies and COI inputs to the data and web services environments to ensure the Authoritative Data Source (ADS), Meta Data, and web-service content are accurate and maintained in support of the Warfighter Mission Domain and the FCBs in accordance with reference t, and JROC approved requirements.

(4) Track, verify and report ADS exposure in accordance with JROC approved requirements.

(5) Lead and/or participate in the appropriate data governance forums to ensure data interoperability within the WMA capabilities in accordance with references t and u.

(6) Ensure data and services are visible, accessible, understandable, interoperable and secure in accordance with reference t.

(7) Through the JROC and DoD CIO, determine compliance of data standards by reviewing the interoperability key performance parameters of capabilities documents required by references l, m, p, u, and w.

d. Enterprise Architecture Development and IT Standards

(1) Ensure, in coordination with the Director, Joint Staff/J-3, USD(AT&L), DoD CIO, the Director, Operational Test and Evaluation (DOT&E), Joint Staff Director for JS J-4, Joint Staff Director for JS J-6, Joint Staff Director for JS J-7, and the DoD Components and in accordance with reference k, that insights gained from combined, joint, and coalition exercises, demonstrations, experiments, and operations are included in JCIDS analysis to facilitate improvements in IT, including NSS interoperability and supportability.

(2) In accordance with references d and k, provide the DoD CIO the joint military priorities for development and selection of IT standards conformance issues.

(3) Lead the development of the Joint Operational Architecture, Command and Control (C2) Joint Mission Threads (JMTs) in accordance with references l and o, 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 w, establish policy and procedures, with 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 in concert with references l and u, and to facilitate the identification of IT, including 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 U.S. Military Forces and, where required, with joint, combined, and coalition forces and with other U.S. Government departments and agencies.

(c) Review, certify, and validate sufficiency of the net readiness-key performance parameters (NR-KPPs) per references l and m.

(d) Support USD(AT&L), DoD CIO and DOT&E, procedures for verification and certification of interoperability based on meeting the requirements of the NR-KPP for new and fielded IT, including NSS throughout a system's life. Enable the establishment of a Coalition Interoperability Assurance and Validation (CIAV) process to support Combatant Commands per references l and n.

(e) Conduct assessments and field analysis of existing and emerging C4 capabilities and systems.

(f) Identify, assess, and approve joint military C4\cyber requirements and establish appropriate operational priority levels.

(g) Through the JROC and DoD CIO, determine compliance of interoperability standards by reviewing the interoperability key performance parameters of capabilities documents required by references l and m. In accordance with references e and m, guide Service architectural development with singular capability and operational views of joint military priorities.

e. Information Assurance (IA) and Cyber Security

(1) In accordance with references e, x, y, z, aa, and ab:

(a) Advocate for Joint Community Cyber Security interests and concerns in DoD joint community boards and forums.

(b) Promulgate comprehensive Cyber Security instructions and guidance for the joint community.

(c) Appoint Combatant Command or Service Authorizing Officials for jointly developed information systems in the WMA, as needed or upon requested.

(d) Advise and assist Combatant Command CIO\Cyber Security Staff with achieving joint community decisions in areas such as enterprise security reciprocity, secure information sharing, connection approval, cross domain solutions, cyber workforce management, security risk management, and achieving security interoperability.

(2) Per reference b, ensure WMA IT portfolio management 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 e, x, y, z, aa, and ab lead development of common network operations tasks for inclusion into the Universal Joint Task List and promulgate associated tactics, techniques and procedures (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.

4. Joint Staff Directorates (J-Dirs) Responsibilities

a. The Joint Staff Director for Command, Control, Communications, and Computers/Cyber (J-6) is also designated the Joint Staff (JS) CIO reporting to the Director, Joint Staff. JS CIO roles and responsibilities, and JS IT portfolio management responsibilities are found in references f and j.

b. The Joint Staff Director for Intelligence (JS J-2) will advocate the JCW CIO interest at the Intelligence Community (IC) CIO Executive Council for intelligence and intelligence-related national security systems (NSS) that support warfighter operations.

c. The Joint Staff Director for Operations (JS J-3) will advocate command, control, communications and computers (C4) requirements and attendant architectural artifacts through the clear delineation of global and regional operational requirements.

d. The Joint Staff Director for Logistics (JS J-4) will advocate Joint Logistics Enterprise (JLEnt) requirements and attendant architectural artifacts

as defined through the Global Combat Support System (GCSS) Planners Board (GO/FO Level Board) through the clear delineation of global and regional logistics requirements.

e. The Joint Staff Director for Logistics (JS J-4) and Joint Staff Director for Force Structure, Resources, and Assessment (JS J-8), represent the NSS and Joint Staff business systems of interest at the Defense Business Committee/ Investment Review Board per reference g.

f. The Joint Staff Director for Joint Force Development (JS J-7) will advocate and enable the Joint Force Development Environment, in support of identified warfighting operational requirements.

g. Joint Staff directorates will use the JCW CIO as a conduit to the DoD CIO Executive Board or JS J-2 for access to the IC CIO Executive Council on issues that involve their functional area and affect the Joint Community. JS J-2 will coordinate with JS J-6/JCW CIO on intelligence systems that impact or interact with operational systems. JCW CIO will advocate IT themes and issues associated with interoperability of major components of the DODIN.

5. Combatant Commands (COCOMs) Responsibilities

a. Combatant Commanders will designate a CIO and develop appropriate guidance for their specific responsibilities in references a, c, e, and h.

b. Combatant Command CIOs may use the JS J-2 as the conduit for issues of intelligence and intelligence-related NSS to the Intelligence Community (IC) CIO Executive Council and should keep the JCW CIO informed.

c. By virtue of their respective transformational roles as assigned in the Unified Command Plan at reference h, Commander, United States Strategic Command (CDRUSSTRATCOM) and Commander, United States Special Operations Command (CDRUSSOCOM) will advocate the following information technology (IT) themes and issues regarding:

(1) Cyberspace Operations – Directing DoD information networks operations and defense. (CDRUSSTRATCOM)

(2) Global Operations against Terrorist Networks – Implementation of transformational capabilities to support global operations against terrorist networks. (CDRUSSOCOM)

(3) “Military Information Support Operations (MISO). (CDRUSSOCOM)

(INTENTIONALLY BLANK)

ENCLOSURE B

REFERENCES

- a. Department of Defense Directive (DoDD) 8000.01, 10 February 2009, "Management of the Department of Defense Information Enterprise"
- b. DoDD 8115.01, 10 October 2005, "Information Technology Portfolio Management"
- c. Section 2223, Chapter 131, of title 10, United States Code
- d. Chairman of the Joint Chiefs of Staff Memorandum (JSM), 29 March 2012, "Reestablishing the Joint Staff J6 Directorate"
- e. DoDD 5144.02, 22 April 2013 "Department of Defense Chief Information Officer (DoD CIO)"
- f. Joint Staff Instruction (JSI) 8000.01 Series, "Joint Staff Chief Information Officer" (not approved for public release)
- g. Department of Defense Chief Information Officer Memorandum, 29 June 2012, "Defense Business Systems Investment Management Process Guidance"
- h. Sections 11103, 11312, and 11313, Chapter 113 of title 40, United States Code
- i. Unified Command Plan, 6 April 2011, with Change-1 dated 12 September 2011
- j. Joint Staff Instruction (JSI) 8130.06, 7 August 2012, "Joint Staff Information Technology (IT) Portfolio Management (PFM)" (not approved for public release)
- k. Joint Staff Notice (JSN) 5110, 3 July 2012, "Information Technology Working Group," 1 (not approved for public release)
- l. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01 Series, "Joint Capabilities Integration and Development System"
- m. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01 Series, "Net Ready Key Performance Parameter (NR KPP)"
- n. Deputy Secretary of Defense Memorandum, 1 July 2013, "Strategic Choices and Management Review Resulting Direction and Guidance"

- o. The Joint Staff Joint Requirements Oversight Council Secretariat Memorandum 026-13, 5 February 2013, “Future Mission Network (Mission Partner Environment), 90-Day Study Report”
- p. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3265.01, 10 November 2013, “Command and Control Governance and Management”
- q. Department of Defense Chief Information Officer Memorandum, July 2012 “Department of Defense Cloud Computing Strategy”
- r. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3150.25 Series, “Joint Lessons Learned Program”
- s. Department of Defense Directive (DoDD) 5100.35, 10 March 1998, “Military Communications-Electronics Board (MCEB)”
- t. Department of Defense Information Enterprise Strategy Plan 2012 to 2012
- u. Department of Defense Instruction (DoDI) 8320.02, 5 August 2013, “Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense”
- v. Department of Defense Directive (DoDD) 4630.5, 5 May 2004 (Certified Current as to 23 April 2007), “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”
- w. Department of Defense Chief Information Officer Memorandum, 10 August 2012, “Department of Defense Information Enterprise Architecture v2.0”
- x. Section 2224 of title 10, United States Code, “Defense Information Assurance Program”
- y. Department of Defense Directive (DoDD) 8500.01E, 24 October 2002 (Current as of 23 April 2007), “Information Assurance (IA)”
- z. Department of Defense 8570.01-Manual, 19 December 2005 (Incorporating Change 3, 24 January 2012), “Information Assurance Workforce Improvement Program”
- aa. CJCSI 8410.02, 8 February 2012, “WMA Principal Accrediting Authority and WMA Authorizing Officials: Policy and Responsibilities”
- ab. Department of Defense Instruction (DoDI) 8510.01, 28 November 2007, DoD Information Assurance Certification and Accreditation Process (DIACAP)

ac. Charter for the Joint Information Environment Management Construct,
9 November 2012

(INTENTIONALLY BLANK)

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

ACAT	Acquisition Category
ADS	Authoritative Data Source
C4	Command, Control, Communications, and Computers
CDRUSSTRATCOM	Commander, United States Strategic Command
CDRUSSOCOM	Commander, United States Special Operations Command
CIO	Chief Information Officer
CIAV	Coalition Interoperability Assurance and Validation
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COI	Community of Interests
CPA	Chairman's Program Assessment
CPIC	Capital Planning and Investment Control
CPM	Capability Portfolio Manager
CPR	Chairman's Program Recommendations
CRA	Chairman's Risk Assessment
DAS	Defense Acquisition System
DITPR	Department of Defense Information Technology Portfolio Repository
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Officer
DoD EA	Department of Defense Enterprise Architecture
DoDIN	Department of Defense Information Network
DOT&E	Director, Operational Test and Evaluation
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy
FCB	Functional Capabilities Board
IC	Intelligence Community
IM	Information Management
IRM	Information Resource Management
IS	Information System
IT	Information Technology
ITCIP	Information Technology Capital Investment Portfolio

J-2	Joint Staff Directorate for Intelligence
J-3	Joint Staff Directorate for Operations
J-4	Joint Staff Directorate for Logistics
J-6	Joint Staff Directorate for Command, Control, Communications, Computers and Cyber/Chief Information Officer
JCA	Joint Capability Area
JCB	Joint Capabilities Board
JCIDS	Joint Capabilities Integration and Development System
JC	Joint Community
JCW CIO	Joint Community Warfighter Chief Information Officer
JIE	Joint Information Environment
JMT	Joint Mission Threads
JROC	Joint Requirements Oversight Council
JS CIO	Joint Staff Chief Information Officer
KM/DS	Knowledge Management/Decision Support
MCEB	Military Communications-Electronics Board
MDR	Meta Data Registry
NCDS	Net-Centric Data Strategy
NCSS	Net-Centric Services Strategy
NR-KPP	Net-Ready Key Performance Parameter
NSS	National Security Systems
PAA	Principal Accrediting Authority
PPBE	Planning, Programming, Budgeting, and Execution
SIPRNET	SECRET Internet Protocol Router Network
TTP	Tactics, Techniques and Procedures
UJTL	Universal Joint Task List
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; unified command. (JP 5-0)

Department of Defense Components. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector general of the Department of Defense, the Department of Defense agencies, field activities, and all other organizational entities in the Department of Defense. (JP 1)

Department of Defense Information Networks (DoDIN) formerly called Global Information Grid (GIG). The globally, interconnected, end-to-end set of information capabilities, associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel including owned and leased communications and computing systems and services, software (including applications, data, security services, and other associated services, and national security systems. (Definition taken from final draft of JP 3-12, Cyberspace Operations. Upon approval of that publication, this term and its definition will be included in JP 1-02)

Department of Defense Enterprise Architecture (DoD IEA). A federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments; and the roadmap for transition to the target environment. (DoDD 8000.01 Reference X)

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 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).

(INTENTIONALLY BLANK)