



CHIEF NATIONAL GUARD BUREAU NOTICE

NG-J6-CIO
DISTRIBUTION: A

CNGB Notice 6200
20 July 2015

JOINT INFORMATION ENVIRONMENT STRATEGIC IMPLEMENTATION GUIDANCE

References: See Enclosure A.

1. Purpose. This notice provides guidance on the National Guard's (NG) transition to the Department of Defense (DoD) Joint Information Environment (JIE) in accordance with (IAW) references a through c. The NG will transition as rapidly as possible with the immediate goal of identifying the most secure, efficient, and cost-effective ways to implement JIE, in coordination with the DoD Components, while continuing to meet the NG's Federal and State mission requirements.

2. Cancellation. None.

3. Applicability. This notice applies to all NG elements.

4. Background.

a. Designing a DoD-wide Information Environment. The JIE is a secure joint information environment comprised of a single cybersecurity architecture, shared information technology (IT) infrastructure, and DoD-wide enterprise services, designed together to increase security, improve mission effectiveness, and achieve IT efficiencies. The JIE is operated and managed using common standards, specifications, and tactics, techniques, and procedures. The JIE initiative results from 2010 Secretary of Defense guidance to consolidate DoD assets into an optimized joint environment for the DoD Components. The NG is required to implement the JIE, excluding any IT infrastructure or services which individual states and territories have purchased exclusively with state funds, are using exclusively in connection with state missions or programs, and do not interface with DoD architectures, infrastructure or services. This requirement to implement JIE is to ensure that critical data, capabilities, and

UNCLASSIFIED

services are protected, available and supportive of unity of command and effort with DoD and non-DoD mission partners.

b. Applicability. The JIE encompasses all DoD IT capabilities (classified and unclassified) used at all operational levels: global, regional or functional, local (to include installations), and tactical (to include incident areas). The JIE supports all mission areas, including NG specific Homeland Defense, Civil Support, and Defense Support of Civil Authorities performed in Title 10 and Title 32 duty status IAW reference e and reference d; and while in State Active Duty status IAW reference g. Specifically, the NG Area of Support (AOS) for JIE is defined as the end users, services, and computing and communications infrastructure where JIE capabilities and services must be implemented to support NGforces as they perform dual Federal and State roles in domestic operations IAW reference f. JIE capabilities and services will enable shared situational awareness through the exchange of operational information among the JFHQs–State and up to the Federal level through the National Guard Bureau IAW references g and h.

c. Implementing the JIE For the NGArea of Support (AOS). The Joint Staff has issued Execute Orders in which the Secretary of Defense directs the DoD-wide global implementation of JIE capabilities and adds NG-specific instructions to support JIE implementation for its AOS. The NG’s implementation objectives include identifying the node designation of all data computing and communications infrastructure within installation-type facilities (for example, armories) of which the Chief of the National Guard (CNGB) is executive agent. The following table provides focus areas, partial descriptions, and samples of high-level implementation objectives that are current as of this notice’s effective date IAW references i and j.

JIE Category	Description	Sample End-State Objectives
Network Normalization	<i>Normalize and consolidate networks using JIE standards, specifications and solutions.</i>	100 percent of planned locations (for example, armories, wings, and units) properly connected to the JIE Wide Area Network (Nonsecure Internet Protocol Router (NIPR) and Secret Internet Protocol Router (SIPR)) per JIE specifications and passing operational traffic.
Security	<i>Implement a single JIE cyber security architecture to protect and share data.</i>	Utilized DoD enterprise perimeter protection (Internet Access Points, Mission Partner Gateways, and Mobility Gateways) and Joint Regional Security Stacks capabilities; established multiprotocol label switching virtual private networks that segregate installation and enterprise traffic.
Enterprise Services	<i>Use DoD-designated enterprise services or request waivers with a required Business Case Analysis.</i>	Utilized DoD Enterprise Directory Services, Defense Enterprise Email, Defense Enterprise Portal Service, enterprise unified capabilities, and more.
Application Rationalization	<i>Identify, categorize, and migrate applications and services to JIE end-state.</i>	Migrated applications and systems to JIE nodes or the commercial cloud, or otherwise retire.
Data Center Consolidation	<i>Consolidate and close data centers under the Federal Data Center Consolidation Initiative.</i>	NGData Centers consolidated and transitioned to Installation Processing Nodes.
Node Transition	<i>Consolidate data computing and communications infrastructure; identify facilities and installations for transition to JIE nodes.</i>	Provided locations for Installation Processing Nodes, Installation Services Nodes, Installation Gateways, and Geographically Separated Units.
Identity and Access Management	<i>Use DoD enterprise capabilities for identity and access management.</i>	Utilized SIPR token and public key infrastructure logon; public key-enabled NIPR and SIPR applications.
Enterprise Licensing	<i>Use enterprise licensing.</i>	Increased number of component-wide, joint, and DoD enterprise licensing agreements.

Table 1. Sample of High-Level Implementation End-State Objectives

5. Action or Procedure. The following actions will support the NG's transition to achieve JIE end-state objectives IAW references k through o.

a. Director of Communications and Chief Information Officer, NG Joint Staff (NG-J6/CIO). The NG-J6/CIO will:

- (1) Serve as the NG transition manager IAW references k and p.
- (2) Oversee the NG's transition to JIE end-state objectives.
- (3) Develop strategic IT concepts, plans, policies, and governance that support the alignment of the NGAOS with JIE end-state objectives.
- (4) Manage joint IT requirements submitted by the NG Joint Staff and the JFHQs-State IAW procedures IAW reference p to ensure JFHQs-State requirements are included in JIE end-state architectures and solutions.
- (5) Advocate for the inclusion of validated joint IT requirements in the JIE Management Construct, DoD Chief Information Officer Executive Board, Joint Requirements Oversight Council, and other DoD-level IT governance forums and planning activities.
- (6) Submit NG-J6/CIO-endorsed NG JIE Node designations to the JIE Management Construct.
- (7) Verify that Army National Guard (ARNG) and Air National Guard (ANG) JIE implementation plans support NG Joint Staff and JFHQs-State requirements and are synchronized with their parent Services and DoD JIE implementation plans.
- (8) Identify NGIT capabilities and assets that contribute to supporting the JIE for the NGAOS.
- (9) Identify issues, risks, and obstacles to JIE transition.
- (10) Communicate the above-referenced assets, issues, risks, and obstacles to the JIE Executive Committee through the JIE Planning and Coordination Cell.
- (11) Validate NGJIE metrics for progress reports.
- (12) Report the NG's JIE progress to the CNGB, the Vice Chief of the National Guard Bureau, and the JIE Management Construct.

b. Army NGCommunications and Automation Directorate (ARNG-G6) and Air NGCommunications Directorate (NGB/A6). The ARNG-G6 and NGB/A6 will:

- (1) Transition to JIE operational and technical end-state objectives.
- (2) Nominate data computing and communication facilities for transition to JIE nodes in coordination with NG-J6/CIO and JFHQs–State.
- (3) Retire IT assets duplicative of JIE capabilities, shared infrastructure, and enterprise services.
- (4) Submit validated Service-specific JIE requirements through parent Service IT requirements, budgeting, and acquisition processes.
- (5) Synchronize NG-specific implementation plans in coordination with the parent Services.
- (6) Identify NGIT capabilities and assets that contribute to supporting the JIE for the NGAOS.
- (7) Identify issues, risks, and obstacles to JIE transition.
- (8) Submit the following to NG-J6/CIO:
 - (a) The above-referenced JIE node nominations, assets, issues, risks, and obstacles.
 - (b) JIE implementation plans and metrics.
 - (c) JIE progress reports.

c. JFHQs–State. The JFHQs–State will:

- (1) Transition to JIE operational and technical end-state objectives.
- (2) Nominate data computing and communication facilities for transition to JIE nodes in coordination with NG-J6/CIO, ARNG-G6, and NGB/A6.
- (3) Retire IT assets duplicative of JIE capabilities, shared infrastructure, and enterprise services.
- (4) Identify NGIT capabilities and assets that contribute to supporting the JIE for the NGAOS.
- (5) Identify issues, risks, and obstacles to JIE transition.

(6) Submit the following to NG-J6/CIO:

(a) The above-referenced JIE node nominations, assets, issues, risks, and obstacles.

(b) JIE implementation plans and metrics.

(c) JIE progress reports.

(d) Joint IT requirements.

6. Releasability. This notice is approved for public release; distribution is unlimited. Copies are available through <<http://www.ngbpd.c.ngb.army.mil>>.

7. Effective Date. This notice is effective on the date signed and will expire one year from the date of signature unless cancelled earlier.



FRANK J. GRASS
General, USA
Chief, National Guard Bureau

Enclosures:

A -- References
GL -- Glossary

ENCLOSURE A

REFERENCES

PART I. REQUIRED

- a. JS Execute Order, 05 December 2012, “DoD Joint Information Environment”
- b. JS Execute Order, 13 September 2013, “Modification–1 to Joint Information Environment Execute Order: Implementation of JIE Increment–1 Capabilities”
- c. JS Execute Order, 12 September 2014, “Modification–2 to Joint Information Environment”
- d. JS Vice Chairman of the Joint Chiefs of Staff Memorandum, 17 July 2014, “Initial Capabilities Document for Joint Information Environment”
- e. DoD Directive 3025.18, 29 December 2010, Incorporating Change 1, 21 September 2012, “Defense Support of Civil Authorities”
- f. JIE Operations Sponsor Group, 18 September 2014, “Joint Information Environment Operations Concept of Operations (CONOPS) Version 2.0”
- g. DoD Directive 5105.83, 05 January 2011, Incorporating Change 1, 30 September 2014, “National Guard Joint Force Headquarters – State”
- h. DoD Directive 5105.77, 21 May 2008, “National Guard Bureau”
- i. DoD Chief Information Officer Memorandum, 20 November 2013, “Joint Information Environment Capability Reporting Metrics”
- j. DoD Chief Information Officer, 07 August 2014, “JIE Metrics, Version 2.0”
- k. DoD Chief Information Office Charter, 09 November 2012, “Charter for the Joint Information Environment Management Construct”
- l. DoD Deputy Secretary of Defense Memorandum, 06 May 2013, “Joint Information Environment Memorandum”
- m. DoD Chief Information Officer Memorandum, 26 September 2013, “Joint Information Environment Implementation Guidance”
- n. DoD Chief Information Officer Memorandum, 22 November 2013, “Component Joint Information Environment Implementation Plans”

o. DoD Chief Information Officer Memorandum, 11 July 2013, “Department of Defense Joint Information Environment: Continental United States Core Data Centers and Application and System Migration”

p. CNGB Instruction 6000.01, 13 August 2012, “National Guard Bureau Joint Information Technology Portfolio Management”

PART II. RELATED

q. DoD Chief Information Office Publication, 06 September 2011, “Department of Defense Information Technology Enterprise Strategy and Roadmap Version 1.0”

r. JS Chairman of the Joint Chiefs of Staff White Paper, 22 January 2013, “Joint Information Environment”