CHIEF NATIONAL GUARD BUREAU INSTRUCTION

NG-J6/CIO
DISTRIBUTION: A

CNGBI 6000.01A
26 September 2016

NATIONAL GUARD BUREAU
JOINT INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT

References: See Enclosure A.

1. Purpose. This instruction establishes policy and assigns responsibilities for the National Guard Bureau (NGB) Joint Information Technology (IT) Portfolio Management (PfM) program in accordance with (IAW) references a through x.

2. Cancellation. This instruction is a revision of CNGBI 6000.01, 13 August 2012, "National Guard Bureau Joint Information Technology Portfolio Management."

3. Applicability. This instruction applies to all elements of the NGB. This instruction does not supersede Army National Guard (ARNG) or Air National Guard (ANG) Service-specific IT governance or IT PfM policies.

4. Policy. It is NGB policy to:

a. Manage Joint IT investments within the National Guard Joint Staff (NGJS) and the Office of the Chief of the National Guard Bureau, regardless of funding.

b. Divide the Joint IT investments portfolio into mission areas containing similar or closely related capabilities supporting NGB and the Department of Defense (DoD), IAW reference a. These missions areas include:

(1) Domestic Operations Mission Area (DOMA). The DOMA supports National Guard (NG) domestic operations.

(2) Business Mission Area (BMA). The BMA supports business operations.

(3) Intelligence Mission Area (IMA). The IMA supports intelligence mission operations.

c. Ensure NGB Joint IT architectures are consistent with DoD command, control, communications, and information-enterprise architecture IAW references i, j, and k.

d. Evaluate Joint IT investments against established outcome-based performance measures to determine improved capability as well as to support changes to the mix of portfolio investments, as necessary IAW reference l.

e. Comply with DoD cybersecurity and Risk Management Framework guidance for Joint IT investments IAW references o and p.

5. Definitions. See Glossary.

6. Responsibilities.

a. Chief of the National Guard Bureau (CNGB). The CNGB will align the NGB's IT investment portfolio with DoD Information Enterprise policies, as required.

b. Director of the National Guard Bureau Joint Staff (DNGBJS). The DNGBJS will serve as the final decision authority for Joint IT investments. The DNGJS may delegate this authority to the NGJS Chief of Staff (NGJS-CoS), as required.

c. NGJS-CoS. The NGJS-CoS will:

(1) Serve as the BMA Lead.

(2) Validate Joint BMA IT requirements by providing an O6 level equivalent signature on the Capability Review Package during the Capability Review Process (see Figure 1).

(3) Serve as the initial approval authority on the best alternative solution for validated Joint BMA IT requirements.

d. Director of Intelligence (NG-J2). The Director of NG-J2 will:

(1) Serve as the IMA Lead.

(2) Validate Joint IMA IT requirements by providing an O6 level equivalent signature on the Capability Review Package during the Capability Review Process (see Figure 1).

(3) Serve as the initial approval authority on the best alternative solution for validated Joint IMA IT requirements.

e. Director of Domestic Operations and Force Development (NG-J3/7). The Director of NG-J3/7 will:

(1) Serve as the DOMA Lead.

(2) Validate Joint DOMA IT requirements by providing an O6 level equivalent signature on the Capability Review Package during the Capability Review Process (see Figure 1).

(3) Serve as the initial approval authority on the best alternative solution for validated Joint DOMA IT requirements.

f. Director of Communications/Chief Information Officer (CIO) (NG-J6/CIO). The Director of NG-J6/CIO will:

(1) Act as the proponent for NGB Joint IT instructions, manuals, notices, and charters, to ensure they are compliant with DoD IT PfM.

(2) Lead the Joint IT Requirements Analysis (JITRA) process and support Investment Review governance processes.

(3) Align NG target IT architecture with DoD IT architecture, as appropriate.

(4) Assist Joint Requirement Sponsors in identifying and evaluating IT solutions, as required.

(5) Maintain the Joint IT Portfolio.

(6) Review Joint IT investments twice during the fiscal year.

(7) Review new and existing Joint IT requirements to ensure Joint IT Requirement Sponsors plan and budget for cybersecurity requirements, IAW reference o.

(8) Ensure NG Joint IT investments are accurately entered into DoD IT investment reporting systems.

(9) Provide IT governance and portfolio management guidance to NGJS system owners.

g. Director of Resource Management and Comptroller (NG-J8). The Director of NG-J8/Comptroller will:

(1) Serve as the Capability Review Process Lead.

(2) Confirm capability gaps and completeness of sponsor documentation by providing O6 level equivalent signature on the Capability Review Package.

(3) Coordinate evaluation of reported shortfalls with the NG-J6/CIO to ensure documented technical information supports the JITRA process.

(4) Provide guidance on the Capability Review Process and Capability Review Package.

h. Chief of NGB Operational Contracting (NGB-OPARC-AQ). The Chief of NGB-OPARC-AQ will:

(1) Refer all Joint IT requirement submissions without a JITRA number to NG-J8 for capability review and requirement validation.

(2) Recommend best procurement approach following the Requirement Sponsor's completion of analysis of alternative solutions.

(3) Provide guidance on acquiring Government-Off-The-Shelf (GOTS) solutions, if a GOTS solution is recommended through the JITRA process.

(4) Support Commercial-Off-The-Shelf (COTS) market research, including Requests for Information, and financial analysis, if a government alternative IT solution is not identified during the JITRA process.

i. Joint IT Requirement Sponsors. Joint IT Requirement Sponsors will:

(1) Coordinate with NG-J8 to evaluate shortfalls through the Capability Review Process.

(2) Determine if confirmed capability gaps can be closed or mitigated by process changes.

(3) Lead analyses of alternatives to identify potential solutions to meet an IT requirement.

(4) Complete total life-cycle cost estimates for IT solutions, as required.

(5) Lead COTS market research and financial analysis to satisfy identified requirements, in the absence of a viable government solution.

(6) Develop IT system architecture IAW reference n.

(7) Use performance measures and attributes to review and evaluate Joint IT investments.

(8) Submit all Joint IT requirements through the JITRA process before submission to the Investment Review process.

(9) Adhere to the Defense Business Council reporting processes for Defense Business Systems with a Future Years Defense Program life-cycle costing more than the amount allowed IAW references e, m, and x.

(10) Coordinate Joint network infrastructure requirements with the ARNG IT Requirements Control Board.

(11) Provide Joint IT project financial, technical, and performance data to support the bi-annual Joint IT portfolio review process.

(12) Report Joint IT investments to the appropriate DoD PfM database(s) IAW references a through e.

j. Director of ARNG-G6 and Director of ANG/A2/3/6. The Directors of ARNG-G6 and ANG/A2/3/6 will:

(1) Support the Capability Review Process, as required.

(2) Support the Joint Portfolio Research process by identifying alternative solutions to meet validated requirements.

(3) Provide expertise to support analyses of alternative solutions.

(4) Provide IT project financial, technical, and performance data to support JITRA processes and Joint IT PfM.

k. Financial Management Board (FMB) Level I. The FMB Level I will:

(1) Prioritize Joint IT investments based on NGB strategic goals and missions.

(2) Execute all chartered Joint IT PfM and oversight functions.

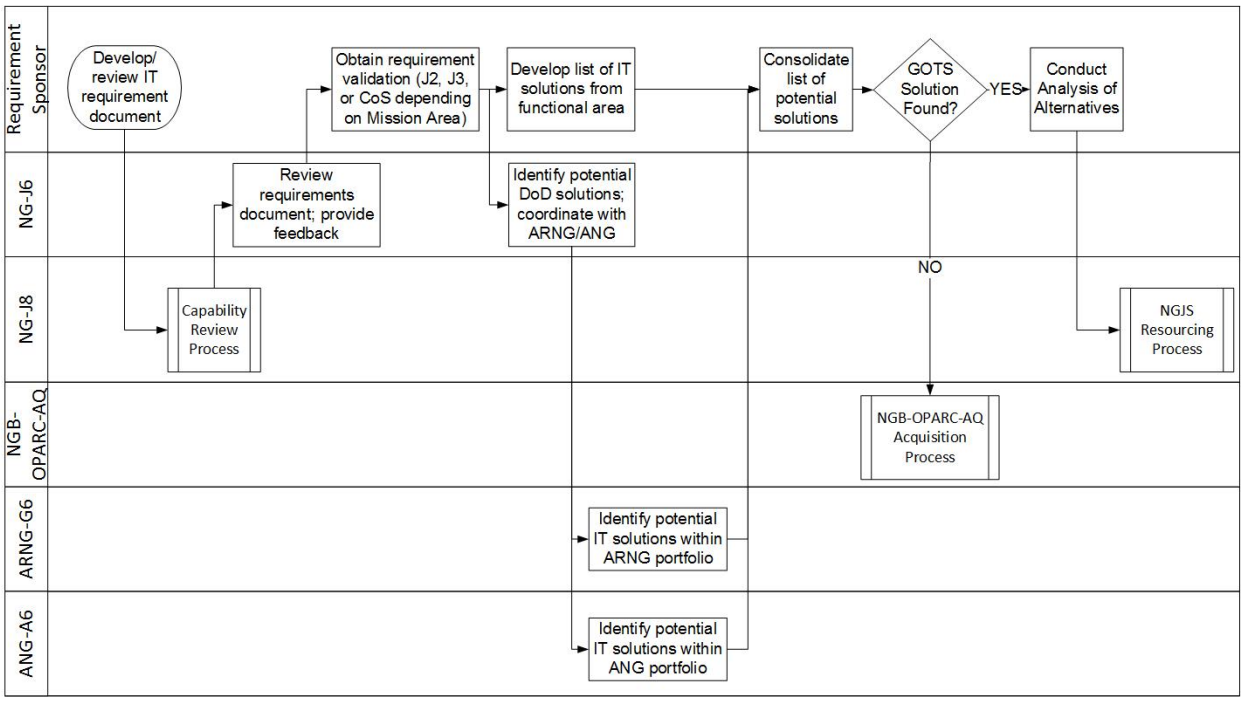

Figure 1. Joint Information Technology Requirements Analysis Process

7. Summary of Changes. This instruction updates mission areas and architecture requirements. Some supporting text for the JITRA process has been removed and inserted into the associated CNGB Manual and Guard Knowledge Online site.

8. Releasability. This instruction is approved for public release; distribution is unlimited. Obtain copies through <http://www.ngbpdc.ngb.army.mil>.

9. Effective Date. This instruction is effective upon publication and must be reissued, cancelled, or certified as current within five years of its publication.

JOSEPH L. LENGYEL
General, U.S. Air Force
Chief, National Guard Bureau

Enclosures:

A -- References
GL -- Glossary

ENCLOSURE A

REFERENCES

PART I. REQUIRED

a. DoD Directive 8115.01, 10 October 2005, "Information Technology Portfolio Management"

b. DoD Instruction 8115.02, 30 October 2006, "Information Technology Portfolio Management Implementation"

c. 40 U.S.C., Subtitle III, Chapters 111, 113, 115 and 117 (formerly division E of the Clinger Cohen Act of 1996)

d. OMB Circular No. A-130, "Management of Federal Information Resources," as amended

e. 10 U.S.C. § 2222, "Defense Business Systems: Architecture, Accountability and Modernization"

f. 10 U.S.C. § 2223, "Information Technology: Additional Responsibilities of Chief Information Officers"

g. 44 U.S.C. § 3506, "Federal Agency Responsibilities"

h. DoD Directive 8000.01, 10 February 2009, "Management of the Department of Defense Information Enterprise"

i. CJCS Instruction 8010.01C, 01 November 2013, "Joint Community Warfighter Chief Information Officer"

j. DoD Directive 7045.20, 25 September 2008, "Capability Portfolio Management"

k. DoD Instruction 8330.01, 21 May 2014, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)"

l. CJCS Instruction 6212.01F, 21 March 2012, "Net Ready Key Performance Parameter (NR KPP)"

m. 10 U.S.C. § 186, "Defense Business System Management Committee"

n. Office of the Deputy Chief Management Officer, Memorandum for Secretaries of the Military Departments, 06 March 2015, "Defense Business Systems Investment Management Process Guidance"

o. DoD Instruction 8500.01, 14 March 2014, "Cybersecurity"

p. DoD Instruction 8510.01, 12 March 2014, "Risk Management Framework (RMF) for DoD Information Technology (IT)"

PART II. RELATED

q. CJCS Instruction 3170.01I, 23 January 2015, "Joint Capabilities Integration and Development System (JCIDS)"

r. JCIDS Manual, 12 February 2015, "Joint Capabilities Integration and Development System (JCIDS)"

s. CJCS Instruction 6510.01F, 09 February 2011, certified current as of 09 June 2015, "Information Assurance (IA) and Support to Computer Network Defense (CND)"

t. Public Law 103-62, 03 August 1993, "Government Performance and Results Act (GPRA)"

u. Public Law 111-352, 04 January 2011, "GPRA Modernization Act of 2010"

v. DoD Directive 5134.01, 09 December 2005, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))"

w. DoD Directive 5000.01, 12 May 2003 and certified as current 20 November 2007, "The Defense Acquisition System"

x. Office of the Deputy Chief Management Officer, February 2015, "Guidance for Review and Certification of Defense Business Systems," Version 3.4

GLOSSARY

PART I. ACRONYMS

ANG	Air National Guard
ARNG	Army National Guard
BMA	Business Mission Area
CIO	Chief Information Officer
CNGB	Chief of the National Guard Bureau
COTS	Commercial-off-the-Shelf
DoD	Department of Defense
DNGBJS	Director of the National Guard Bureau Joint Staff
DOMA	Domestic Operations Mission Area
FMB	Financial Management Board
GOTS	Government-Off-The-Shelf
IAW	In accordance with
IMA	Intelligence Mission Area
IT	Information Technology
IT PfM	Information Technology Portfolio Management
JITRA	Joint Information Technology Requirements Analysis
NGJS-CoS	National Guard Joint Staff Chief of Staff
NG-J2	Directorate of Intelligence
NG-J3/7	Directorate of Domestic Operations and Force Development
NG-J6/CIO	Directorate of Communications and CIO
NG-J8/Comptroller	Directorate of Resource Management and Comptroller
NGB	National Guard Bureau
NGJS	National Guard Joint Staff
NGB-OPARC-AQ	National Guard Bureau Operational Contracting
PfM	Portfolio Management
PM	Program Manager

PART II. DEFINITIONS

Analysis of Alternatives -- Evaluation of the performance, operational effectiveness, operational suitability, cybersecurity requirements and estimated costs of alternative systems under consideration to fill a mission capability gap.

Business Mission Area -- Comprised of investments supporting National Guard administrative functions such as: acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management.

Capability -- The ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks. It is defined by an operational user and expressed in broad operational terms in the format of a joint or initial capabilities document or a joint doctrine, organization, training, materiel, leadership and education, personnel, and facilities change recommendation.

Capability Review -- A process for determining if an operational or business gap must be filled, and, if so, whether this gap is best reduced or eliminated using non-materiel solutions, existing systems, or materiel solutions.

Capability Requirement -- A requirement to meet an organization's roles, functions, and missions in current or future operations.

Domestic Operations Mission Area -- Supports National Guard Domestic Operations and aligns most closely with the Department of Defense's Warfighter Mission Area.

Gaps -- The inability to perform an assigned mission.

Enterprise Architecture -- Defines: a) the people, processes, and technology required in the "current" and "target" environments, and b) the roadmap for transition to the target environment in accordance with reference c.

Information Technology -- Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency in accordance with reference a.

Intelligence Mission Area -- Supports National Guard Intelligence Operations and aligns most closely with the Department of Defense's Intelligence Mission Area.

Interoperability -- The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

IT Investment -- The development and sustainment resources needed in support of information technology or information technology-related initiatives. These resources include, but are not limited to research, development, test and evaluation appropriations; procurement appropriations; personnel appropriations; and operations and maintenance appropriations. Information technology investment recommendations focus on whether acquisition programs, information technology systems (as discussed in reference h),

models and simulations, and budget initiatives should be initiated, modified, continued, or terminated. Specific financial or budget information will support program, system, and initiative recommendations. Information technology investments covered by this policy include both defense business systems and national security systems in accordance with reference g.

IT Portfolio Management -- The management of information technology investments using strategic planning, risk balancing, architectures, and outcome-based performance measures to achieve strategic capability objectives. Information technology portfolio elements are evaluated according to outcome performance measures. Management activities for the portfolio include strategic planning, capital planning, governance, process improvements, performance metrics or measures, requirements generation, acquisition and development, and operations in accordance with reference h.

IT Requirement Sponsor -- Any National Guard Bureau organization (Office of the Chief of the National Guard Bureau, National Guard Joint Staff, Army National Guard, and Air National Guard directorates) submitting an information technology capability necessary to fulfill or prevent a gap in executing National Guard domestic operations missions, intelligence missions, or supporting business functions.

Joint Integration Team -- An integrated product team supporting the Joint Information Technology Requirements Analysis process by performing Joint Portfolio Review and other Information Technology Portfolio Management duties.

Joint Information Technology Requirement -- An information technology capability needed to fulfill or prevent a gap in executing National Guard domestic operations missions, intelligence missions or supporting business functions.

Materiel Solution -- An information technology solution adopted, developed, or purchased to satisfy one or more capability requirements or needs that may reduce or eliminate one or more capability gaps.

Mission Area -- A defined area of responsibility with functions and processes that contribute to mission accomplishment.

Non-materiel Solution -- Changes to doctrine, organization, training, (existing) materiel, leadership and education, personnel, and/or facilities, implemented to satisfy one or more capability requirements (or needs) and reduce or eliminate one or more capability gaps, without the need to develop or purchase a new materiel solution.

Requirement -- A gap that leadership validated, and wants to expend the effort to close.

Shortfall -- A perceived inability to perform a mission.

Standard -- Quantitative or qualitative measures for specifying the levels of performance of a task.

Sustainment -- The provision of personnel, training, logistics, environment, safety, and occupational health management, and other support required to maintain availability of materiel and support operations or combat until successful accomplishment or revision of the mission or the national objective.

Validation -- The review of documentation by an operational authority other than the user to confirm the requirement to close a gap for an operational capability.

Validation authority -- The individual within the Department of Defense components charged with overall capability definition and validation of requirements.