CHIEF OF THE NATIONAL GUARD BUREAU INSTRUCTION

NGB-J6 CNGBI 6000.01B
DISTRIBUTION: A 24 May 2021

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 o.

2. Cancellation. This instruction cancels and replaces its previous edition, CNGBI 6000.01A, 26 September 2016, "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 IT investments within the National Guard Bureau Joint Staff (NGBJS) and the Office of the Chief of the National Guard Bureau.

b. Manage the NGB Joint Staff (NGBJS) IT investment portfolio in alignment with Department of Defense (DoD) mission areas containing similar or closely related capabilities supporting NGB and DoD IAW reference a. These mission areas include:

(1) Warfighting Mission Area. The Warfighting Mission Area provides life cycle oversight to applicable DoD Component and Combatant Commander IT investments (programs, systems, and initiatives). The NGB manages the Domestic Operations Mission Area (DOMA) as a subset of the Warfighting Mission Area. The DOMA supports the National Guard's execution of domestic operations and defense support of civil authorities.

(2) Business Mission Area. The Business Mission Area supports business operations and ensures that the right capabilities, resources, and materiel are reliably

delivered to our warfighters: what they need, where they need it, when they need it, anywhere in the world.

(3) Defense Intelligence Mission Area. The Defense Intelligence Mission Area includes IT investments within the Military Intelligence Program and Defense component programs of the National Intelligence Program. The Under Secretary of Defense for Intelligence has delegated responsibility for managing the Defense Intelligence Mission Area portfolio to the Director of the Defense Intelligence Agency, but the Under Secretary of Defense for Intelligence retains the final signature authority. Defense Intelligence Mission Area management will require coordination among portfolios that extend beyond the DoD to the overall intelligence community.

(4) Enterprise Information Environment Mission Area. IAW reference c, this mission area includes computing infrastructure for the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DoD enterprise hardware, software operating systems, and hardware/software support that enables the DoD Information Network.

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 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 reference o.

5. Definitions. See Glossary.

6. Responsibilities.

a. Chief of the National Guard Bureau (CNGB). The CNGB is responsible for all NG IT initiatives (for example, Information Sharing Environment), expeditionary executive communications, incident awareness and assessment, etc.

b. Directors of the ARNG, ANG, and NGB Space Operations. The Directors of ARNG, ANG, and NGB Space Operations will:

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

(2) Support the Joint portfolio research process by identifying alternative solutions to meet approved NGBJS IT requirements.

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

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

c. NGB Director of Staff. The NGB Director of Staff will serve as the decision authority for Joint IT investments. The NGB Director of Staff may delegate this authority to the NGB Chief Information Officer.

d. NGBJS Chief of Staff. The NGBJS Chief of Staff will:

(1) Serve as the NGB Business Mission Area lead.

(2) Serve as the approving authority for verifying Joint Business Mission Area IT requirements by providing an O-6-level-equivalent signature on the JITRA form during the Capability Review Process.

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

e. Director of Joint Intelligence (NGB-J2). The Director of NGB-J2 will:

(1) Serve as the NGB Defense Intelligence Mission Area lead.

(2) Serve as the approving authority for verifying NGB intelligence and counterintelligence IT requirements and investments by providing an O-6-level-equivalent signature on the JITRA form after the Capability Review Process.

(3) Endorse incident awareness and assessment IT capabilities that integrate into DOMA IT requirements and investments.

f. Director of Operations (NGB-J3/4/7). The Director of NGB-J3/4/7 will:

(1) Serve as the NGB DOMA lead.

(2) Serve as the approving authority for verifying Joint DOMA IT requirements and investments by providing an O-6-level-equivalent signature on the JITRA form after the Capability Review Process.

(3) Serve as the approving authority for verifying Joint DOMA requirements and investments that include the common operating picture, shared situational awareness, and incident awareness and assessment capabilities.

(4) Serve as the initial approval authority on the best alternative solution for validated Joint Warfighting Mission Area and DOMA IT requirements.

g. NGB Director of C4 Systems and Chief Information Officer (NGB-J6). The Director of the NGB-J6 will:

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

(2) Lead the JITRA process for all new or significantly changed IT capabilities.

(3) Align Joint National Guard 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) Conduct Joint IT reviews annually.

(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 National Guard Joint IT investments are accurately entered into DoD IT investment reporting systems.

(9) Provide IT governance and portfolio management guidance to NGBJS system owners and IT investment leads.

(10) Facilitate the Chief Information Officer Executive Council to support the CNGB's oversight of National Guard IT investment matters.

(11) Review NGBJS-requested National Guard and Reserve Equipment Account-funded IT capabilities for aligning with CNGB priorities and DOMA investment guidance.

h. Director of Programs and Resources/Comptroller (NGB-J8). The Director of NGB-J8 will:

(1) Serve as the Capability Review Process lead.

(2) Confirm capability gaps and completeness of sponsor documentation by providing O-6-level-equivalent signature on the JITRA form.

(3) Coordinate evaluation of reported shortfalls with the NGB-J6 to ensure documented technical information aligns with the JITRA process.

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

i. Director of Acquisitions and Head of the Contracting Activity (NGB-AQ/HCA). The NGB-AQ/HCA will:

(1) Ensure all IT-related NGBJS contract or Military Interdepartmental Purchase Request actions have been reviewed by NGB-J6 and have been issued a JITRA number. Refer all Joint IT requirement submissions that do not have a JITRA number to the NGB-J8 for capability review and requirement validation.

(2) Support best procurement approaches after the Requirement Sponsor has completed an analysis of alternative solutions.

(3) Provide guidance on acquiring government-off-the-shelf solutions, if a government-off-the-shelf solution is recommended during the JITRA process.

(4) Provide assistance, if requested, for commercial-off-the-shelf market research, including requests for information, if a government alternative IT solution is not identified during the JITRA process.

j. Joint IT Requirement Sponsors (from NGBJS Directorates). Joint IT Requirement Sponsors will:

(1) Coordinate with NGB-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 commercial-off-the-shelf 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) Coordinate Joint network infrastructure requirements with the ARNG IT Requirements Control Board.

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

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

(12) Support annual IT investment review activities by providing requested information to the NGB-J6.

7. Summary of Changes. This instruction provides more information on NGB's alignment to DoD Mission Areas. It also assigns greater responsibility for the Warfighting Mission Area to the NGB-J3/4/7.

8. Releasability. This instruction is approved for public release; distribution is unlimited. It is available at <https://www.ngbpmc.ng.mil>.

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

DANIEL R. HOKANSON
General, USA
Chief, National Guard Bureau

Enclosures:

A -- References
GL -- Glossary

ENCLOSURE A

REFERENCES

PART I. REQUIRED

a. Department of Defense (DoD) Directive 5105.77, 30 October 2015, "National Guard Bureau (NGB)," Incorporating Change 1, 10 October 2017

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

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

d. Title 40 United States Code (U.S.C.), Subtitle III, Chapters 111, 113, 115, and 117 (formerly Division E of the Clinger Cohen Act of 1996)

e. Office of Management and Budget Circular No. A-130, "Managing Information as a Strategic Resource," as amended 28 July 2016

f. 10 U.S.C. § 2222, "Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management"

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

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

i. DoD Directive 8000.01, 17 March 2016, "Management of the Department of Defense Information Enterprise (DoD IE)," Incorporating Change 1, 27 July 2017

j. Chairman of the Joint Chiefs of Staff (CJCS) Instruction 8010.01C, 01 November 2013, "Joint Community Warfighter Chief Information Officer"

k. DoD Directive 7045.20, 25 September 2008, "Capability Portfolio Management," Incorporating Change 2, 21 June 2019

l. DoD Instruction 8330.01, 21 May 2014, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," Incorporating Change 2, 11 December 2019

m. Office of the Deputy Chief Management Officer, Memorandum for Secretaries of the Military Departments, 10 May 2019, "Defense Business Systems Investment Management Process Guidance," <https://cmo.defense.gov/Resources/Defense-Business-Council-and-Investment-Management/> (last accessed on 24 May 2021)

n. DoD Instruction 8500.01, 14 March 2014, "Cybersecurity," Incorporating Change 1, 07 October 2019

o. DoD Instruction 8510.01, 12 March 2014, “Risk Management Framework (RMF) for DoD Information Technology (IT),” Incorporating Change 3, 29 December 2020

PART II. RELATED

p. CJCS Instruction 5123.01H, 31 August 2018, “Charter of the Joint Requirements Oversight Council (JROC) and the Implementation of the Joint Capabilities Integration and Development System”

GLOSSARY

PART I. ACRONYMS

ANG	Air National Guard
ARNG	Army National Guard
CNGB	Chief of the National Guard Bureau
DoD	Department of Defense
DOMA	Domestic Operations Mission Area
FMB	Financial Management Board
IAW	In accordance with
IT	Information Technology
IT PfM	Information Technology Portfolio Management
JITRA	Joint Information Technology Requirements Analysis
NGB	National Guard Bureau
NGB-J2	Joint Intelligence Directorate
NGB-J3/4/7	Operations Directorate
NGB-J6	C4 Systems and Chief Information Officer Directorate
NGB-J8	Programs and Resources/Comptroller Directorate
NGB-AQ/HCA	Office of Acquisitions and Head of the Contracting Activity
NGBJS	National Guard Bureau Joint Staff
PfM	Portfolio Management

PART II. DEFINITIONS

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 Gap -- The inability to perform an assigned mission.

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.

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

Enterprise Architecture -- The people, processes, and technology required in the "current" and "target" environments, and 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.

Information Technology Investment -- The development and sustainment resources needed in support of information technology or information technology-related initiatives. These resources include 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 (in accordance with 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.

Information Technology 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.

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

Defense Intelligence Mission Area -- Includes information technology investments within the Military Intelligence Program and Defense component programs of the National Intelligence Program.

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, 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 -- The lack of forces, equipment, personnel, materiel, or capability, reflecting the difference between the resources identified as a plan requirement and those quantities identified as apportioned for planning that would adversely affect the command's ability to accomplish its mission.

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

Sustainment -- The provision of logistics and personnel services required to maintain and prolong operations until successful mission accomplishment.

Validation -- The review and approval of capability requirement documents by a designated validation authority. The Joint Requirements Oversight Council is the ultimate validation authority for capability requirements unless otherwise delegated to a subordinate board or to a designated validation authority in a Service, Combatant Command, or other Department of Defense component.