CHIEF NATIONAL GUARD BUREAU INSTRUCTION

NG-J6/CIO
DISTRIBUTION: A

CNGBI 6001.00
28 February 2017

NATIONAL GUARD BUREAU CYBERSECURITY PROGRAM

References: See Enclosure B.

1. Purpose. This instruction establishes policy and assigns responsibilities for the National Guard Bureau (NGB) Cybersecurity Program in accordance with (IAW) references a, b, c, and d.

2. Cancellation. None.

3. Applicability. This instruction applies to personnel who have management or security responsibilities over National Guard Joint Staff (NGJS) Information Technology (IT) systems. This instruction does not supersede any Army National Guard (ARNG) or Air National Guard (ANG) IT cybersecurity policies.

4. Policy. It is NGB policy to use the Risk Management Framework (RMF) and the Department of Defense (DoD) Enterprise Mission Assurance Support Service (eMASS) tool to facilitate the Assessment and Authorization process for all Joint IT Systems, which are Information Systems (IS) or Platform IT (PIT) that reside in the NGJS or the Office of the Chief of the National Guard Bureau (OCNGB,) IAW reference c.

a. Joint IT Systems. Joint IT systems must be registered in the DoD Information Technology Portfolio Repository (DITPR) IAW references b, e, and f, to provide senior DoD decisionmakers coherent and contextual views of capabilities to support the certification process for the various Investment Review Boards and the Defense Business Systems Management Committee.

b. DoD Cybesecurity Scorecard. Compliance with DoD Cybersecurity Scorecard reporting requirements must be maintained by consolidating and reporting cybersecurity metrics through DoD CyberScope IAW reference g. This web application automates the collection of cybersecurity survey data submitted by components of the DoD and several other organizations to consolidate their data into one survey.

c. Mission Areas. Personnel who monitor cybersecurity risks must gather information by assesing the following mission areas.

MISSION AREA	COVERAGE
NGB Domestic Operations Mission Area (DOMA)	Includes three additional mission areas to include Homeland Defense, National Guard Civil Support, and the National Guard Baseline Operating Posture.
NGB Business Mission Area (BMA)	Includes business and financial management infrastructure—processes, systems, and data standards—and the integration of business transformation for the DoD business enterprise.
NGB Intelligence Mission Area (IMA)	Includes IT investments within the Military Intelligence Program and Defense component programs of the National Intelligence program.

Table 1. Mission Areas

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes. This is the initial publication of CNGBI 6001.00.

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 every five years.

JOSEPH L. LENGYEL
General, USAF
Chief, National Guard Bureau

Enclosures:

A -- Responsibilities
B -- References
GL -- Glossary

ENCLOSURE A

RESPONSIBILITIES

1. Chief of the National Guard Bureau (CNGB). The CNGB will:

a. Provide strategic cybersecurity IT guidance and direction to the NG.

b. Appoint an Authorizing Official for the NGJS and OCNGB IAW reference c.

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

a. Provide oversight for the NGB Cybersecurity Program.

b. Assist NGJS and OCNGB Information System Owners (ISO) with cybersecurity responsibilities throughout the Joint IT Requirements Analysis process.

c. Collaborate with mission area leads to identify NGB operational requirements.

d. Assign cybersecurity responsibilities to the NGB Program Manager (PM), Systems Manager (SM) and ISO IAW references b and c.

e. Appoint a NGB Senior Information Security Officer (SISO) IAW references b and c.

f. Notify the CNGB of cybersecurity portfolio risks IAW reference c.

g. Ensure NGB Joint IT systems are categorized according to the guidelines provided in reference c.

h. Address cybersecurity risks and requirements throughout the IT life cycle for Joint IT investments within the NGJS portfolio IAW reference b.

i. Verify certification and qualification standards are met by the NGJS and OCNGB cybersecurity workforce IAW reference h.

j. Monitor Joint IT system compliance with DoD and Federal reporting requirements IAW references i through z.

k. Assist mission area leads by monitoring cybersecurity risks within the NGB BMA, DOMA, and IMA.

3. NGJS SISO. The NGJS SISO will:

a. Administer the NGB Cybersecurity Program.

b. Serve as the primary NGJS point of contact for the RMF Technical Advisory Group IAW reference aa.

c. Advise the Authorizing Official on risk acceptance for Joint IT systems.

d. Provide guidance on security control identification and approval.

e. Coordinate the collection, aggregation, and reporting of required (ARNG/ANG/NGJS/OCNGB) metrics, security posture, and pertinent information for overall NGB Cybersecurity Scorecard reporting to DoD.

f. Educate NGB privileged users of Joint IT systems on individual accountability and cybersecurity awareness.

g. Review and manage the NGB instance within the eMASS tool.

h. Review Joint IT entries in DITPR for accuracy.

i. Assess effectiveness of security controls for Joint IT systems.

j. Manage the DoD CyberScope submission process for NGB.

4. Authorizing Official. The Authorizing Official will:

a. Evaluate cybersecurity risks against NG mission objectives IAW reference c.

b. Authorize Joint IT systems and coordinate with the required Authorizing Officials and System Owners IAW references b.

c. Comply with Authorizing Official qualification requirements IAW references b and c.

5. NGJS-Chief of Staff (NGJS-CoS). The NGJS-CoS will:

a. Monitor cybersecurity risks across NGB BMA IAW reference bb.

b. Appoint a PM or SM to oversee NG IT, IS and PIT systems within the NGJS BMA.

6. Office of the NGB Principal Assistant for Contracting (NGB-OPARC). NGB-OPARC will receive a memorandum from NG-J6/CIO certifying all NGB Joint IT procurement acquisition packet documents incorporate cybersecurity requirements IAW references b, c, and bb.

7. Director of Manpower and Personnel (NG-J1). The Director of NG-J1 will coordinate with the CIO to ensure all NGJS cybersecurity positions are properly documented with position descriptions and responsibilities.

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

a. Monitor and mitigate cybersecurity risks across the Joint portion of IMA IAW IT portfolio management program guidance.

b. Appoint a PM or SM to oversee Joint IT systems within the NGJS IMA.

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

a. Monitor and mitigate cybersecurity risks across NGB DOMA IAW IT portfolio management program guidance.

b. Appoint a PM or SM to oversee Joint IT systems within the NGB DOMA.

c. Coordinate cybersecurity training with the ARNG and ANG.

d. Ensure NGB Cybersecurity exercise coordination with the ARNG and ANG, Interagency and Interorganizational mission partners.

10. NGJS and OCNGB ISO. The NGJS and OCNGB ISOs will:

a. Monitor and mitigate IT risks during the acquisition process and the system's life cycle IAW references b, c, and bb.

b. Allocate personnel and financial resources as authorized within their respective programs to satisfy NGB Cybersecurity Program compliance requirements, IAW reference b, c, and bb.

c. Appoint Information System Security Managers (ISSM) and Information System Security Officers (ISSO) to IT, IS and PIT systems.

d. Document and report ISSM and ISSO certifications to the NGJS SISO, IAW references c, h, and cc.

e. Register and report IT systems into eMASS and DITPR IAW references c and e.

11. PM or SM. The PM or SM will accomplish program or system objectives for the development, production, and sustainment of the user's operational needs.

12. ISSM. The ISSM will:

a. Secure enterprise information by designing, implementing, and enforcing security controls, safeguards, policies, and procedures.

b. Manage their respective staff.

ENCLOSURE B

PART I. REQUIRED

a. DoD Directive 5105.77, 30 October 2015, "National Guard Bureau (NGB)"

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

c. DoD Instruction 8510.01, 12 March 2014, Incorporating Change 1, 24 May 2016, "Risk Management Framework (RMF) for DoD Information Technology (IT)"

d. CNGB Memorandum, 05 June 2015, "Appointment of Chief Information Officer (CIO) for National Guard Joint Staff (NGJS) Information Technology"

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

f. DoD Instruction 5015.02, 24 February 2015, "DoD Records Management Program"

g. OMB Memorandum M-16-03, 03 October 2015, "Fiscal Year 2015-2016 Guidance on Improving Federal Information Security and Privacy Management Requirements"

h. DoD Directive 8140.01, 11 August 2015, "Cyberspace Workforce Management"

i. CJCS Instruction 6211.02D, 24 January 2012, "Defense Information System Network (DISN) Responsibilities"

j. CJCS Instruction 6510.01F, 09 February 2011, "Information Assurance (IA) and Support to Computer Network Defense (CND)"

k. CJCS Manual 6510.01B, 10 July 2012, "Cyber Incident Handling Program"

l. DoD Chief Information Officer (CIO) Memorandum, 17 January 2012, "DoD Commercial Mobile Device (CMD) Interim Policy"

m. DoD Directive 8100.02, 14 April 2004, "Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)"

n. DoD Instruction 5205.13, 29 January 2010, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA Activities)

o. DoD Instruction 8420.01, 03 November 2009, “Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies”

p. DoD Instruction 8520.02, 24 May 2011, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling”

q. DoD Instruction 8520.03, 13 May 2011, “Identity Authentication for Information Systems”

r. DoD Directive O-8530.1, 07 March 2016, “Support to Computer Network Defense (CND)”

s. DoD Instruction 8551.01, 28 May 2014, “Ports, Protocols, and Services Management (PPSM)”

t. DoD Instruction 8580.1, 09 July 2004, “Information Assurance (IA) in the Defense Acquisition System”

u. DoD Instruction 8582.01, 06 June 2012, “Security of Unclassified DoD Information on Non-DoD Information Systems”

v. NIST Special Publication 800-37, February 2010, “Guide to Applying the Risk Management Framework to Federal Information Systems”

w. NSTISSP No. 11, July 2003, “National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products”

x. DHS FY-15 CIO Annual FISMA Metrics v1.3, 30 July 2015

y. DA Pam 220-1, 16 November 2011, “Department of Defense Readiness Reporting System”

z. DoD Directive 7730.65, 11 May 2015, “Department of Defense Readiness Reporting System-Army Procedures”

aa. DoD Risk Management Framework (RMF) Technical Advisory Group (TAG) Charter, 14 October 2014

bb. CNGB Instruction 6000.01, 13 August 2012, “National Guard Bureau (NGB) Joint Information Technology Portfolio Management”

cc. DoD Manual 8570.01-M, 19 December 2005: Incorporating Change 4, 10 November 2015, “Information Assurance Workforce Improvement Program”

PART II. RELATED

dd. DoD Directive 5000.01, 12 May 2003, "The Defense Acquisition System"

ee. DoD Manual 7000.14-R, September 2015, "DoD Financial Management Regulation: Volume 2B, Chapter 18: "Information Technology (Including Cyberspace Operations)"

ff. Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 239, 30 November 2015, "Acquisition of Information Technology,"

gg. Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 208.74, 20 April 2015, "Enterprise Software Agreements"

GLOSSARY

PART I. ACRONYMS

ANG	Air National Guard
ARNG	Army National Guard
BMA	Business Mission Areas
CIO	Chief Information Officer
CNGB	Chief of the National Guard Bureau
DoD	Department of Defense
DOMA	Domestic Operations Mission Area
DITPR	Department of Defense Information Technology Portfolio Repository
eMASS	Enterprise Mission Assurance Support Service
IA	Information Assurance
IAW	In accordance with
IMA	Intelligence Mission Areas
IS	Information System
ISO	Information System Owner
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
NG	National Guard
NGB	National Guard Bureau
NGB-OPARC	Office of the Principal Assistant Responsible for Contracting
NGJS	National Guard Joint Staff
NGJS-CoS	National Guard Joint Staff Chief of Staff
NG-J1	Directorate of Manpower and Personnel
NG-J2	Directorate of Intelligence
NG-J6/CIO	Directorate of Communications and Chief Information Officer
NG-J3/7	Directorate of Domestic Operations and Force Development
OCNGB	Office of the Chief of the National Guard Bureau
PIT	Platform Information Technology
PM	Program Manager
RMF	Risk Management Framework
SISO	Senior Information Security Officer
SM	Systems Manager

PART II. DEFINITIONS

Information System -- An integrated set of components for collecting, storing, and processing data that provides information, knowledge, and digital products.

Joint IT System -- The Information Systems or Platform Information Technology that reside in the National Guard Joint Staff or the Office of the Chief of the National Guard Bureau.

Platform Information Technology -- Computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

Risk Management Framework -- The unified information security framework for the entire Federal Government that replaced the legacy Certification and Accreditation processes within Federal Government departments and agencies, the Department of Defense, and the Intelligence Community.

eMASS -- A service-oriented web application that supports Information Assurance program management and automates the Department Information Assurance Certification and Accreditation Process and Risk Management Framework.

DoD Information Technology Portfolio Repository -- The central repository for Information Technology system information to support the certification processes of the various Investment Review Boards and the Defense Business Systems Management Committee.