CHIEF OF THE NATIONAL GUARD BUREAU INSTRUCTION

NGB-J3/4/7 CNGBI 2202.01
DISTRIBUTION: A 08 November 2021

NATIONAL GUARD OPERATIONS SECURITY PROGRAM

References: See Enclosure B.

1. Purpose. This instruction establishes policy and assigns responsibilities for the National Guard (NG) Operations Security (OPSEC) Program in accordance with (IAW) the references.

2. Cancellation. None.

3. Applicability. This instruction applies to the National Guard Bureau (NGB) and NG IAW reference c. Nothing in this instruction will be read to limit or change Chief of the National Guard Bureau (CNGB) responsibilities as outlined in reference c. NG personnel, units, or equities assigned to or otherwise supporting other Military Departments will follow the OPSEC programs associated with those Military Departments.

4. Policy. It is NG policy to protect all NG, supported Department of Defense (DoD), and supported Interagency missions, functions, programs, and activities IAW references a and b.

a. OPSEC is the pinnacle security program that integrates all security functions to safeguard critical and sensitive information and protect DoD missions, functions, programs, and activities.

b. OPSEC will be integrated across the entire spectrum of NG missions, functions, programs, and activities. This includes coordinating across the NGB; the States, Territories, and District of Columbia NG Joint Force Headquarters-State (JFHQs-State); DoD OPSEC programs; and other State and Federal agencies to protect critical and sensitive information.

c. The level of OPSEC is dependent on the threat, vulnerability, and risk to the assigned mission, function, program, or activity, and available resources.

d. NG personnel shall maintain essential control of information that allows adversaries and potential adversaries to plan, prepare, and conduct military and other

operations against the United States, which includes safeguarding such information from unauthorized access and disclosure.

e. The NG OPSEC Program will employ OPSEC countermeasures to deny adversaries and potential adversaries any indicators that may reveal critical or sensitive information about NG missions and functions.

f. NG OPSEC and other security and information operations programs will be closely coordinated to account for force protection and the security of information and activities.

g. The Army National Guard of the United States, Air National Guard of the United States, and National Guard Bureau Space Operations (NGB-SO), under the direction of the Director of the Army National Guard (DARNG), Director of the Air National Guard (DANG), and the Director of NGB-SO, respectively, will integrate NG OPSEC procedures to support both the NG OPSEC Program and those associated with the Military Departments.

h. The Office of the Chief of the National Guard Bureau and the NGB Joint Staff, under the direction of the CNGB and the NGB Director of Staff, respectively, will integrate NG OPSEC procedures to support the NG OPSEC Program.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes. None. This is the initial publication of CNGBI 2202.01.

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 signature and must be revised, reissued, canceled, or certified as current every five years.

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

Enclosures:

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

ENCLOSURE A

RESPONSIBILITIES

1. CNGB. The CNGB will:

a. Maintain NG readiness by establishing and maintaining a comprehensive NG OPSEC Program IAW references a and b.

b. Appoint the Director of Operations, NGB-J3/4/7 as the Senior Official to establish and manage the NG OPSEC Program.

c. Designate, train, and resource an OPSEC coordinator for the Office of the Chief of the National Guard Bureau to support the NG OPSEC Program as a member of the NG OPSEC Program Working Group.

2. DARNG, DANG, and Director of NGB-SO. The DARNG, DANG, and Director of the NGB-SO will:

a. Program, plan, budget, and execute NG OPSEC requirements within the budgets of the Army National Guard of the United States and the Air National Guard of the United States.

b. Develop OPSEC policies, plans, procedures, and guidelines with OPSEC Program requirements to enhance NG readiness.

c. Integrate OPSEC training and exercise requirements in operational plans and orders to validate consistency with the established guidance.

d. Designate, train, and resource an OPSEC coordinator to support the NG OPSEC Program as members of the NG OPSEC Program Working Group.

e. Provide oversight and manage installation OPSEC responsibilities IAW DoD and Service policy and guidance.

f. Coordinate initiatives that impact this effort with the NG OPSEC Program Manager.

g. Nest NG OPSEC procedures to support both the NG OPSEC Program and those associated with the Military Departments.

3. NGB Director of Staff. The NGB Director of Staff will:

a. Designate a Resource Management Officer to review funding strategies to meet the NG OPSEC Program resource requirements for training support, certification requirements, and exercises for NGB staff during the budget execution year.

b. Oversee and manage NG wide OPSEC responsibilities IAW DoD and Service policy and guidance.

c. Through the NG OPSEC Program Manager, publish the NGB OPSEC Plan.

d. Publish a charter for the NG OPSEC Program Working Group to provide means for deliberate and purposeful coordination among members, stakeholders, and leadership.

4. Director of Operations (NGB-J3/4/7). Director of NGB-J3/4/7 is the office of primary responsibility for the NG OPSEC Program and designates the NG Continuity Program Manager as the NG OPSEC Program Manager.

5. NGB Joint Staff Directorates. NGB Joint Staff Directorates will appoint OPSEC coordinators to the OPSEC Program Working Group to ensure directorate equities are considered and to provide subject matter recommendations as necessary to guide policy and program implementation, maintenance, evaluation, and improvement.

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

a. Support the planning and programming of resource requirements for the NG OPSEC Program.

b. Assist the DARNG, DANG, and Director, NGB-SO in the development of funding strategies to meet the NG OPSEC Program resource requirements for the 54 NG JFHQs-State during the budget execution year.

7. The Adjutants General and the Commanding General of the District of Columbia. The Adjutants General and Command General of the District of Columbia will appoint an OPSEC coordinator as the point of contact for the NG OPSEC Program to:

a. Ensure the minimum standards in references a and b are met within the constraints defined by their State, Territory, or District of Columbia's law and policy.

b. Ensure that information sharing with the NG OPSEC Program complies with both Federal and their State, Territory, or District of Columbia's law and policy.

c. Ensure that access to OPSEC Program information is strictly limited to authorized individuals with the proper security clearance and need to know.

d. Ensure that all individuals granted access to OPSEC Program information have completed training IAW references a and b and any additional training prescribed by the NG OPSEC Program.

e. Ensure that written protocols establish the standards for referring an OPSEC compromise incident to supervisors, law enforcement agents, counterintelligence agencies, and the NG OPSEC Program.

f. Ensure that NG JFHQs-State activities comply with Service OPSEC program requirements IAW Federal and State law, and are integrated with the NG OPSEC Program.

8. NG OPSEC Program Manager. The NG OPSEC program manager will:

a. Serve as the principal official for NG OPSEC matters and chair the NG OPSEC Program Working Group.

b. Integrate OPSEC processes in all activities and operations that prepare, sustain, or employ the Armed Forces during war, crisis, or peace including, but not limited to, special access programs, DoD contracting, international agreements, force protection, domestic operations, and release of information to the public.

c. Oversee the NG OPSEC Program to promote an understanding and practice of OPSEC among all elements of the NG.

d. Appoint a full-time NG OPSEC coordinator to help oversee the NG OPSEC Program.

e. Identify critical and sensitive information and develop policies and procedures for its protection.

f. Ensure compliance with policy for content reviews of information intended for release outside the control of the organization, including release to the public, is appropriately evaluated during program reviews and other oversight activities IAW references a and b.

g. Confirm guidance is established that requires OPSEC planning be integrated into the planning, development, and implementation stages of net-centric programs and operating environments, and that data aggregation concerns are assessed and risk-management strategies applied IAW references a and b.

h. Ensure establishment, execution, and evaluation of OPSEC awareness, education, and training programs are consistent with Service Instructions and Regulations.

i. Comply with additional duties and responsibilities IAW reference a.

9. NG OPSEC Coordinator. The NG OPSEC coordinator will:

a. Develop, communicate, and ensure implementation of standards, policies, and procedures that supplement this instruction and meet the specific needs of NG personnel.

b. Identify necessary resources for the effective implementation of the NG OPSEC Program.

c. Conduct program reviews to evaluate and assess the effectiveness and efficiency of the NG OPSEC Program.

d. Establish an internal NGB process to report disclosures of critical and sensitive information through appropriate channels and implement mitigating actions.

e. Verify OPSEC support capabilities are utilized for program development and review, planning, training, surveys, assessments, and related support, as required.

f. Ensure OPSEC is coordinated and integrated with NG JFHQs-State and other Federal, State, and local government agencies, operations, and activities as appropriate.

g. Confirm policies and procedures are established for the review of unclassified information for OPSEC considerations and data aggregation prior to public release IAW references a and b.

h. Ensure other NG OPSEC coordinators, information operations professionals, public affairs personnel, contracting specialists, counterintelligence professionals, and personnel responsible for the review and approval of information intended for public release have received specialized OPSEC training for their duties IAW references a and b.

i. Publish guidance to ensure that NG unclassified and classified contract requirements properly reflect OPSEC responsibilities and that those responsibilities are included in contracts when applicable.

j. Comply with additional duties and responsibilities IAW reference a.

10. Subcomponent OPSEC Coordinators. The OPSEC coordinators at the subcomponent levels as designated by commanders and directors will fulfill their duties and responsibilities IAW this instruction and reference a.

ENCLOSURE B

REFERENCES

PART I. REQUIRED

a. Department of Defense (DoD) Manual 5205.02-M, 03 November 2008, "DoD Operations Security (OPSEC) Program Manual," Incorporating Change 2, 29 October 2020

b. DoD Directive 5205.02E, 20 June 2012, "DoD Operations Security (OPSEC) Program," Incorporating Change 2, 20 August 2020

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

d. 5 United States Code Section 552a, "The Privacy Act of 1974," As amended, 30 April 2021

PART II. RELATED

e. National Security Decision Directive Number 298, 22 January 1988, "National Operations Security Program"

f. DoD Manual 5200.01, Volume 1, 24 February 2012, "DoD Information Security Program: Overview, Classification, and Declassification," Incorporating Change 2, 28 July 2020

g. DoD Manual 5200.01, Volume 2, 24 February 2012, "DoD Information Security Program: Marking of Information," Incorporating Change 4, 28 July 2020

h. DoD Manual 5200.01, Volume 3, 24 February 2012, "DoD Information Security Program: Protection of Classified Information," Incorporating Change 3, 28 July 2020

i. DoD Manual 5220.22-M, 28 February 2006, "National Industrial Security Program Operating Manual," Incorporating Change 2, 18 May 2016

j. Secretary of Defense Memorandum, 25 January 2011,"Strategic Communication and Information Operations in the DoD"

k. Office of the Chairman of the Joint Chiefs of Staff, June 2020, "DoD Dictionary of Military and Associated Terms"

l. Chairman of the Joint Chiefs of Staff Instruction 3213.01D, 07 May 2012, "Joint Operations Security"

m. Army Regulation 530-1, 26 September 2014, “Operations Security”

n. Air Force Instruction 10-701, 24 July 2019, “Operations Security (OPSEC),” Incorporating Change 1, 09 June 2020

o. Chief National Guard Bureau Instruction 2402.00, 19 April 2019, “National Guard Information Security Program and Protection of Sensitive Compartmented Information”

GLOSSSARY

PART I. ACRONYMS

CNGB	Chief of the National Guard Bureau
DANG	Director of the Air National Guard
DARNG	Director of the Army National Guard
DoD	Department of Defense
IAW	In accordance with
NG	National Guard
NGB	National Guard Bureau
NGB-J3/4/7	Operations Directorate
NGB-J8	Programs and Resources/Comptroller Directorate
NGB-SO	National Guard Bureau Space Operations
NG JFHQs-State	National Guard Joint Force Headquarters-State
OCNGB	Office of the Chief of the National Guard Bureau
OPSEC	Operations Security

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this instruction.

Countermeasure -- Anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

Critical Information -- Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

Indicator -- Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities.

Operations Security -- A process of identifying critical information and analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators and vulnerabilities that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries and determine which of these represent an unacceptable risk; then select and execute countermeasures that eliminate the risk to friendly actions and operations or reduce it to an acceptable level.

Operations Security Assessment -- An evaluative process of an organization, operation, activity, exercise, or support function to determine if sufficient countermeasures are in place to protect critical information.

Operations Security Plan -- A plan that provides the organization a living document that can be used to implement the appropriate countermeasures given the mission, assessed risk, and resources available to the unit. Operations Security plans generally take two forms; both should be updated as circumstances and personnel change over time. An Operations Security operations plan provides specific countermeasures to be applied in a specific operation. It may be generated as an annex to a Joint Operation Planning and Execution System plan or as a local document endorsed by the commander. An Operations Security program plan provides guidelines for implementation of routine procedures and measures to be employed during daily operations or activities of a given unit. The plan should be endorsed by the unit commander.

Operations Security Process -- A process that examines a complete activity to determine what, if any, exploitable evidence of classified or sensitive activity may be acquired by adversaries. It is an analytical, risk-based process that incorporates five distinct elements: Critical Information Identification, Threat Analysis, Vulnerability Analysis, Risk Assessment, and Operations Security Countermeasures.

Operations Security Program Manager -- A full-time appointee or primary representative assigned to develop and manage an Operations Security program.

Operations Security Survey -- An application of the Operations Security process by a team of subject matter experts to conduct a detailed analysis of activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries.

Risk -- A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

Risk Assessment -- A process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss.

Risk Management -- The process of identifying, assessing, and controlling risks by making decisions that balance risk costs with mission benefits. Costs may be measured in financial cost, loss of assets, loss of information, or loss of reputation.

Sensitive Information -- Information that the loss, misuse, unauthorized access, or modification of which could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled in accordance with reference d, but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of National defense or foreign policy.

Threat Analysis -- A process that examines an adversary’s technical and operational capabilities, motivation, and intentions, designed to detect and exploit vulnerabilities.

Vulnerability Analysis -- A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity.