



CHIEF NATIONAL GUARD BUREAU INSTRUCTION

NGB-J2
DISTRIBUTION: A

CNGBI 2500.00
18 July 2018

NATIONAL GUARD BUREAU INSIDER THREAT PROGRAM

References: See Enclosure A.

1. Purpose. This instruction establishes policy and assigns responsibilities for the National Guard Bureau (NGB) Insider Threat (InT) Program in accordance with (IAW) reference a.
2. Cancellation. None.
3. Applicability. This instruction applies to personnel assigned to the NGB and to the 54 National Guard (NG) Joint Force Headquarters-State (NG JFHQs-State).
4. Policy. It is NGB policy to prevent, deter, detect, and mitigate actions by malicious insiders who present a threat to national security or NG personnel, facilities, operations, and resources IAW reference a. This instruction identifies training, education and awareness requirements for NG personnel and contractors IAW references b and c. NGB must meet the minimum standards for Executive Branch Insider Threat Programs IAW references d, e, f, and g through the NGB InT Program.
 - a. Coordination. The NGB InT Program will coordinate among NG elements across the 54 States, Territories, and District of Columbia, Department of Defense (DoD) information systems, and other Federal agencies to mitigate the risks of malicious insiders.
 - b. Training. NG military and civilian personnel, contractors, and volunteers who have access to DoD resources must be trained, educated, and aware of InT information IAW reference c. NGB InT Program personnel must be trained in:

UNCLASSIFIED

(1) Counterintelligence (CI) and security fundamentals, to include applicable legal issues.

(2) NGB procedures for InT response action(s).

(3) Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information.

(4) Applicable civil liberties and privacy laws, regulations, and policies.

(5) Investigative referral requirements IAW reference c, as well as other policy or statutory requirements that mandate referrals to an internal entity, such as a security office or NGB Inspector General Office, or external investigative entities such as the Federal Bureau of Investigation, the Department of Justice, or military investigative service.

c. Compliance. NGB military and civilian personnel, contractors, and volunteers must comply with all applicable laws and DoD policy issuances, including those regarding whistleblowers, civil liberties, intelligence oversight, and privacy protections.

d. Personally Identifiable Information (PII). PII will be assessed IAW references h, i, and j. United States persons information (USPI) that constitutes intelligence will also be handled IAW references k, l, m, and n.

(1) Comply with reference n for activities related to the NGB InT Program, including information sharing and collection. Information on individuals and organizations not affiliated with the DoD will not be acquired unless allowed pursuant to references o and p.

(2) Handle Personally Identifiable Health Information IAW references q, r, s, t, u, and v.

5. Definitions. See Glossary.

6. Responsibilities.

a. Chief of the National Guard Bureau (CNGB). The CNGB will appoint a Senior Official IAW reference b, to manage the NGB-InT Program and establish a process to gather, integrate, and centrally analyze, and respond to CI, security, Information Assurance, Human Resources, law enforcement (LE), and other information indicative of a potential InT.

b. Director of the Army National Guard (DARNG) and Director of the Air National Guard (DANG). The DARNG and the DANG will:

(1) Appoint, in writing, an official from their respective Service component to serve as the Program Manager to manage and oversee that Service component's Insider Threat Program IAW references a through e.

(2) Ensure compliance with the minimum requirements set forth in references a through e and establish a reporting channel which includes the NGB InT Senior Official and the NGB InT Hub.

c. NGB InT Program Senior Official. The NGB InT Program Senior Official will appoint an NGB InT Program Manager to:

(1) Manage the NGB InT Program and maintain relationships with outside agencies.

(2) Provide resource recommendations to CNGB.

(3) Develop and promulgate a comprehensive NGB InT procedural guidance.

(4) Submit to CNGB an NGB InT implementation plan and an annual NGB InT Program report thereafter regarding the progress or status. At a minimum, the annual reports will document annual accomplishments, resources allocated, insider threat risks to the NG, recommendations and goals for program improvement, and major impediments or challenges.

(5) Ensure the NGB InT Program is developed and implemented in consultation with the Office of the NGB Chief Counsel, records management, civil liberties, and privacy officials so all NGB InT Program activities, to include training, are conducted IAW applicable laws, whistleblower protections, and civil liberties and privacy policies.

(6) Establish oversight mechanisms and procedures to ensure all NGB InT Program personnel are trained in handling USPI.

(7) Establish guidelines and procedures for the retention of records and documents necessary to complete assessments required by references a and e.

(8) Facilitate NGB InT Program reviews by CNGB-designated officials to ensure compliance with United States laws, as well as legal and civil liberty protections.

(9) Establish a group of NGB personnel from each directorate to form the NGB InT Hub for communication and analysis of potential InTs to the NGB.

(10) Establish procedures for a multi-disciplinary threat management capability, comprised of analysts trained by a National InT Task Force accredited course.

(11) Establish threat management capability IAW reference n, and all other applicable laws and DoD policies.

(12) Ensure the threat management capability includes an ability to share relevant LE, civilian, and military personnel management, mental health, cybersecurity, security, and CI information with commanders, directors or civilian equivalents throughout NGB.

(13) Require that information from subject matter experts be shared with and provided to the NGB InT Hub from LE, CI, mental health, security, civilian and military personnel management, legal, and cybersecurity.

(14) Establish NGB InT Program management forums to monitor implementation of reference a.

(15) Verify NGB InT Program implementation and policy conformance by contractors and other non-DoD entities that have authorized access to DoD resources as required by contract or agreement pursuant to references o and p.

(16) Incorporate InT education and awareness into annual CI Awareness and Reporting training IAW reference c.

(17) Provide a representative for departmental and interagency forums engaged in countering InTs.

(18) Provide information to the Under Secretary of Defense for Intelligence for the report listed in reference b.

(19) Ensure NGB LE policies and operating procedures address the information-sharing requirements prescribed in references a and w.

d. The Adjutants General (TAG) and the Commanding General of the District of Columbia (CG). TAGs and the CG will appoint a representative as a point of contact for the NGB InT Hub.

e. NG JFHQs-State InT Representatives. NG JFHQs-State InT Representatives will:

(1) Ensure that the minimum standards in reference b are met within the constraints defined by their State, District, or Territory's law and policy.

(2) Ensure that information sharing with the NGB complies with both

Federal and their State, District, or Territory's law and policy.

(3) Ensure that access to all Insider Threat Program information is strictly limited to authorized individuals with a need to know.

(4) Ensure that all individuals granted access to Insider Threat Program information have completed at a minimum insider threat, privacy, and counterintelligence familiarity training prescribed by the NGB InT Program and signed an InT Non-Disclosure Agreement (NDA).

(5) Ensure that NG JFHQs-State InT Programs have access to advice from law enforcement, security, counterintelligence, personnel counseling, and (when possible) mental health counseling professionals within the State or Territory National Guard organization. Subject matter experts will be trained according to para (4) above and sign an NDA before having access to PII related to any inquiry.

(6) Ensure that written protocols establish the standards for referring an inquiry for action to supervisors, human resource offices, law enforcement agents, or counterintelligence agencies. No referral for action will occur without preliminary review and approval by TAGs or by their designated representative (O6 or above).

(7) Ensure that InT information be retained IAW the DoD Systems of Records Notice within any additional constraints imposed by State or Territory law and regulation.

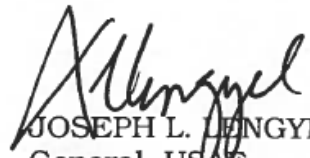
(8) Ensure that State, District and Territory ARNG and ANG activities are complying with Service InT program requirements in accordance with Federal and State law.

7. Summary of Changes. This is the initial publication of CNGBI 2500.00.

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

18 July 2018

9. Effective Date. This instruction is effective upon signature and must be reissued, cancelled or certified as current within five years from the date signed.



JOSEPH L. LENGYEL
General, USAF
Chief National Guard Bureau

Enclosures:

A -- References

GL -- Glossary

ENCLOSURE A

REFERENCES

- a. DoD Directive 5205.16, 30 September 2014, "The DoD Insider Threat Program," Incorporating Change 2, 28 August 2017
- b. Presidential Memorandum, 21 November 2012, "National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs"
- c. DoD Directive 5240.06, 17 May 2011, "Counterintelligence Awareness Reporting (CIAR)," Incorporating Change 2, 01 July 2017
- d. Executive Order 13526, 29 December 2009, "Classified National Security Information"
- e. Executive Order 13587, 07 October 2011, "Structural Reforms to Improve Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"
- f. Public Law (P.L.) 112-81 Section 922, 31 December 2011, "National Defense Authorization Act for Fiscal Year 2012"
- g. Committee on National Security Systems Directive (CNSSD) No. 504, 30 September 2016, "Directive on Protecting National Security Systems from Insider Threat"
- h. Title 5 United States Code (U.S.C.) Section 552a, 07 January 2011, "The Privacy Act of 1974"
- i. DoD Directive 5400.11, 08 May 2007, "DoD Privacy Program," Incorporating Change -1 September 2011
- j. DoD Directive 5400.11-R, 14 May 2007, "Department of Defense Privacy Program"
- k. DoD Manual 5240.01, 08 August 2016, "Procedures Governing the Conduct of DoD Intelligence Activities"
- l. CNGB Instruction 2000.01B, 04 April 2017, "National Guard Intelligence Activities"
- m. CNGB Manual 2000.01, 26 November 2012, "National Guard Intelligence Activities"

- n. DoD Instruction 1000.29, 17 May 2012, "DoD Civil Liberties Program," Incorporating Change 1, 26 November 2014
- o. DoD Directive 5200.27, 07 January 1980, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense"
- p. CNGB Instruction 2400.00 Change 1, 07 November 2013, "Acquisition and Storage of Information Concerning Persons and Organizations not Affiliated with the Department of Defense"
- q. P.L. 104-191, 21 August 1996 "Health Insurance Portability and Accountability Act of 1996"
- r. Code of Federal Regulations, Title 45, §§ 160, 162, and 164, 15 January 2009, "Public Welfare"
- s. DoD Instruction 6490.04, 04 March 2013, "Mental Health Evaluations of Members of the Military Services"
- t. DoD Instruction 6490.08, 17 August 2011, "Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members"
- u. DoD Directive 6025.18-R, 01 January 2003, "DoD Health Information Privacy Regulation"
- v. DoD Directive 8580.02-R, 12 July 2007, "DoD Health Information Security Regulation"
- w. Executive Order 12333, 04 December 1981, "United States Intelligence Activities"
- x. 5 U.S.C. § 105, "Executive Agency"
- y. 5 U.S.C. § 102, "Military Departments"
- z. 5 U.S.C. § 104, "Independent Establishment"

GLOSSARY

PART I. ACRONYMS

ANG	Air National Guard
ARNG	Army National Guard
CI	Counterintelligence
CG	Commanding General of the District of Columbia
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
IA	Information Assurance
IAW	In accordance with
InT	Insider Threat
LE	Law Enforcement
NG	National Guard
NGB	National Guard Bureau
NG JFHQs-State	National Guard Joint Force Headquarters-State
PII	Personally Identifiable Information
TAG	The Adjutants General
USPI	U.S. Person Information

PART II. DEFINITIONS

Classified Information -- Sensitive information to which access is restricted by law or regulation to a particular class of people. A formal security clearance is required to handle classified documents or access classified data. The clearance process requires a favorable background investigation.

Counterintelligence -- Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

Counterintelligence Awareness and Reporting -- Training conducted by certified professionals to ensure the awareness of and preparedness for, the threats of malicious insiders and Foreign Intelligence Entities.

Employee -- A person, employed by, detailed or assigned to, a department or agency in accordance with references x, y, and z.

Insider -- Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.

Insider Threat -- The danger of damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, workplace violence, sabotage, or the loss or degradation of departmental resources or capabilities by personnel with authorized access.

Senior Official -- Designated person principally responsible for establishing a process to gather, integrate, centrally analyze, and respond to counterintelligence, security, information assurance, human resource, law enforcement, and any other relevant information indicative of a potential insider threat.

User Activity Monitoring -- The monitoring and recording of user actions including the use of applications, windows opened, system commands executed, check boxes clicked, text entered/edited, URLs visited and nearly every other on-screen event to protect data by ensuring that employees and contractors are staying within their assigned tasks, and posing no risk to the organization.

Workplace Violence -- Any act or threat of physical violence, harassment, intimidation, or other threatening disruptive behavior that occurs at the worksite.