



# CHIEF NATIONAL GUARD BUREAU INSTRUCTION

NGB-J2  
DISTRIBUTION: A

CNGBI 2402.00  
15 April 2019

## NATIONAL GUARD INFORMATION SECURITY PROGRAM AND PROTECTION OF SENSITIVE COMPARTMENTED INFORMATION

References: See Enclosure B.

1. Purpose. This instruction establishes policy and assigns responsibilities for the National Guard (NG) Information Security (INFOSEC) Program in accordance with (IAW) references a through q.
2. Cancellation. This instruction cancels and replaces Chief of the National Guard Bureau (CNGB) Notice 2402, 21 December 2017, "National Guard Information Security Program," and CNGB Instruction 2200.01, 16 November 2015, "National Guard Access to Top Secret Sensitive Compartmented Information."
3. Applicability. This instruction applies to all National Guard Bureau (NGB) and NG joint elements as defined in references p, r, and s. States, Territories, and the District of Columbia are hereafter referred to as "States." National Guard Bureau Joint Staff (NGBJS) Directorates at the Temple Army National Guard Readiness Center, Air National Guard Readiness Center, and National Guard Joint Directorates at the Pentagon are hereafter referred to as an "Activity."
4. Policy. It is NG policy to classify, safeguard, and declassify national security information IAW references a through d. Identify and safeguard controlled unclassified information (CUI) IAW reference e. Declassification of information will receive the same attention as the classification of information so that information remains classified only as long as required by national security.
  - a. Do not classify, maintain as classified, fail to declassify, or designate as CUI any information to:
    - (1) Conceal violations of law, inefficiency, or administrative error.

**UNCLASSIFIED**

- (2) Prevent embarrassment to a person, organization, or agency.
- (3) Restrain competition.

b. Release information that does not require protection in the interests of national security or as required by statute or regulation.

c. Reduce the volume of classified national security information and CUI, in whatever format or media, to the minimum necessary to meet operational requirements.

d. Access to classified information provided to NG personnel and contractors under United States Code Title 5, Title 10, Title 50, Title 32 and DoD Manual 5220.22 does not apply to State Active Duty (SAD) status. If personnel in a SAD status require access to classified information, The Adjutant General (TAG) or the Commanding General of the District of Columbia (CG) will request access approval from a sponsoring Federal agency IAW references l and m.

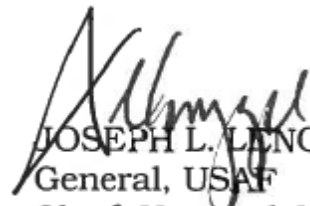
e. Process, store, use, or discuss sensitive compartmented information (SCI) only in an accredited SCI facility (SCIF). The NGB will certify and accredit, in writing, all joint element classified open storage areas in the NGB and the States IAW references l and m.

f. Manage DoD Special Access Programs IAW reference j. NGB training programs will emphasize security requirements and responsibilities for protecting classified information and CUI from unauthorized disclosure, pursuant to references a through d, i, and l. All locally developed initial and refresher NG INFOSEC training must meet the minimum standards outlined in references b through e. The NGBJS, Joint Intelligence Directorate (NGB-J2), Information Security Branch (NGB-J24), developed training that meets these standards and is available for use by INFOSEC staff with responsibilities outlined in this instruction.

g. Implement safeguarding requirements and incident response measures addressing willful, negligent, and inadvertent mishandling of classified information IAW reference f. Leaders and supervisors at all levels must consider and, at their discretion, take appropriate administrative, judicial, contractual, or other corrective or disciplinary action to address negligent disclosures of classified information commensurate with the seriousness of the security violation.

h. The CNGBI, TAGs, CG, and their designated staff have ready access to SCI within one hour's travel of their primary duty location. If a SCIF is not accessible within one hour's travel of the NG Joint Force Headquarters-State (NG JFHQs-State), TAGs or the CG may establish a SCIF through minor construction or refit of an existing facility.

5. Definitions. See Glossary.
6. Responsibilities. See Enclosure A.
7. Summary of Changes. This is the initial publication of CNGBI 2402.00.
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 revised, 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. CNGB. The CNGB will:

- a. Protect classified information and CUI from unauthorized disclosure consistent with reference i.
- b. Appoint, in writing, an NG Senior Activity Official (SAO) IAW reference a.
- c. Appoint, in writing, an NG Senior Intelligence Official (SIO) IAW reference g.

2. SAO. The SAO will appoint, in writing, the NGBJS Activity Security Manager (ASM) IAW reference b and direct, administer, and oversee the NG INFOSEC Program IAW references b through e, including:

- a. Classification, declassification, and safeguarding of classified information.
- b. Security education and training programs.
- c. Implementation of reference i.

3. NGB SIO. The NGB SIO will:

- a. Appoint, in writing, an NGB Special Security Officer (SSO) IAW reference g.
- b. Ensure adequate funding and effective implementation of the NG SCI Security Program, including awareness and education, IAW references g through i.
- c. Coordinate with the NGB SAO, as appropriate, to achieve a consistent and cohesive NG INFOSEC Program.

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

- a. Appoint, in writing, an ASM to properly manage and oversee their respective Service component INFOSEC Program IAW references b through e and Service-specific regulations.
- b. Appoint, in writing, a senior leader (O-6 or Government Grade-15 or above) to properly oversee their SCI Program IAW references g through i and Service-specific regulations.

c. Establish an Activity INFOSEC reporting channel in conjunction with Service-specific reporting requirements that include the CNGB, NGB SAO, and NGB SIO IAW references b through e and i.

d. Ensure compliance with Activity INFOSEC Program requirements IAW references b through e and i.

5. NGBJS Directors. The NGBJS Directors will appoint, in writing, at least one Security Assistant (SA) to oversee their Directorate's INFOSEC Program under the functional authority of the NGB-J24 IAW references b through e.

6. TAG. TAGs will:

a. Appoint, in writing, at least one primary and one alternate SA to oversee the NG JFHQs-State Joint Staff INFOSEC Program under the functional authority of the NGB IAW references b through e.

b. Ensure all NG SCIFs within their States have an assigned SSO or Special Security Representative (SSR).

c. Ensure their respective NG JFHQs-State INFOSEC Program is managed and implemented IAW references b through e, g through i, l, and m, as supplemented by CNGB Issuances.

7. ASM. The ASM will:

a. Manage and implement the NG INFOSEC Program on behalf of the CNGB, DARNG, or DANG IAW reference b. ASMs have direct access to their respective senior leader.

b. Ensure all activities, organizations, directorates, and offices under their security purview comply with the Information Security Oversight Office annual self-inspection checklist reporting requirements.

c. Appoint SAs, as necessary.

d. Appoint an Assistant ASM (AASM), as necessary.

8. AASM. The AASMs will assist with NG INFOSEC Program implementation, maintenance, and local oversight. AASMs report directly to their ASMs.

9. SA. The SAs perform daily administrative security functions under the direction of the ASM or AASM. The SAs will:

a. Serve as the first line of defense against security incidents.

b. Conduct and track initial and annual NG INFOSEC training.

c. Gather data related to the Information Security Oversight Office and report it to the ASM.

d. Coordinate with other security leadership as required.

10. NGB SSO. The NGB SSO will:

a. Manage the NG SCI Program and oversee SCI security functions for the NGBJS, including oversight of NGBJS SCIFs.

b. Support and oversee the NG JFHQs-State SCI Program and oversee SCI security functions for the NG JFHQs-State, including oversight of SCIFs that primarily support the NG JFHQs-State. This includes ensuring assigned SSOs and SSRs are properly trained.

c. Provide support to the Activity SCI Programs as requested or as directed by the NGB SIO.

11. Activity SIOs. The Activity SIOs will:

a. Appoint, in writing, an Activity SSO to ensure adequate funding and effective implementation of the Activity SCI Program, including awareness and education, IAW references g through i.

b. Coordinate with the specific ASM, as appropriate, to achieve a consistent and cohesive Activity INFOSEC Program.

12. Activity SSOs. The Activity SSOs will:

a. Manage the Activity SCI Program and oversee SCI security functions for their Activity, including all requirements outlined in reference g.

b. Support and oversee the Activity SCI Program within the States related to their specific Activity, including any SCIFs that are primarily force structure for their respective Service. This includes ensuring assigned SSOs and SSRs are properly trained.

13. SSOs and SSRs. The SSOs and SSRs within the States will provide NG JFHQs-State SCI Program oversight and management for their respective SCIF under the functional authority of the NGB IAW references g through i.

ENCLOSURE B

REFERENCES

PART I. REQUIRED

- a. DoD Instruction 5200.01, 21 April 2016 (as amended), "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," Incorporating Change 1, 01 May 2018
- b. DoD Manual 5200.01, Volume 1, 24 February 2012, "DoD Information Security Program: Overview, Classification, and Declassification," Incorporating Change 1, 04 May 2018
- c. DoD Manual 5200.01, Volume 2, 24 February 2012, "DoD Information Security Program: Marking of Classified Information," Incorporating Change 2, 19 March 2013
- d. DoD Manual 5200.01, Volume 3, 24 February 2012, "DoD Information Security Program: Protection of Classified Information," Incorporating Change 2, 19 March 2013
- e. DoD Manual 5200.01, Volume 4, 24 February 2012, "DoD Information Security Program: Controlled Unclassified Information (CUI)," Incorporating Change 1, 09 May 2018
- f. Deputy Secretary of Defense Memorandum, 14 August 2014, "Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Systems"
- g. DoD Manual 5105.21, Volume 1, 19 October 2012, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security," Incorporating Change 1, 16 May 2018
- h. DoD Manual 5105.21, Volume 2, 19 October 2012, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security," Incorporating Change 1, 05 April 2018
- i. DoD Manual 5105.21, Volume 3, 19 October 2012, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities," Incorporating Change 1, 05 April 2018
- j. DoD Directive 5205.07, 01 July 2010, "Special Access Program (SAP) Policy," Incorporating Change 1, 31 August 2018

- k. Executive Order 13526, 29 December 2009, “Classified National Security Information”
- l. 32 Code of Federal Regulations, Parts 2001 and 2003, 25 June 2010, “Classified National Security Information Implementing Directive; Final Rule”
- m. Executive Order 13549, 18 August 2010, “Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities”
- n. Department of Homeland Security Implementing Directive, February 2012, “Classified National Security Program for State, Local, Tribal, and Private Sector Entities”
- o. Executive Order 13556, 04 November 2010, “Controlled Unclassified Information”
- p. DoD Directive 5105.77, 30 October 2015, “National Guard Bureau (NGB),” incorporating Change 1, 10 October 2017
- q. Intelligence Community Directive 703, 21 June 2013, “Protection of Classified National Intelligence, Including Sensitive Compartmented Information”
- r. DoD Directive 5105.83, 05 January 2011, “National Guard Joint Force Headquarters–State (NG JFHQs-State),” Incorporating Change 1, 30 September 2014
- s. CNGB Instruction 1001.01, 29 June 2016, “National Guard Joint Force Headquarters–State”

## PART II. RELATED

- t. Intelligence Community Directive 705, 26 May 2010, “Sensitive Compartmented Information Facilities”
- u. Intelligence Community Standard 705.1, 17 September 2010, “Physical and Technical Security Standards for Sensitive Compartmented Information Facilities”
- v. Intelligence Community Standard 705.2, 17 September 2010, “Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information”
- w. Intelligence Community Technical Specification for Intelligence Community Directive/Intelligence Community Standard 705, 28 September 2017, “Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.4”



x. DoD Instruction 5205.11, 6 February 2013, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," Incorporating Change 1, 31 August 2018

## GLOSSARY

### PART I. ACRONYMS

AASM	Assistant Activity Security Manager
ASM	Activity Security Manager
CG	Commanding General of the District of Columbia
CNGB	Chief of the National Guard Bureau
CUI	Controlled unclassified information
DANG	Director of the Air National Guard
DARNG	Director of the Army National Guard
DoD	Department of Defense
IAW	In accordance with
INFOSEC	Information security
JFHQs	Joint Force Headquarters
NG	National Guard
NGB	National Guard Bureau
NGB-J2	Joint Intelligence Directorate
NGB-J24	Information Security Branch
NGBJS	National Guard Bureau Joint Staff
NG JFHQs-State	National Guard Joint Force Headquarters–State
SA	Security Assistant
SAD	State Active Duty
SAO	Senior Activity Official
SCI	Sensitive compartmented information
SCIF	Sensitive compartmented information facility
SIO	Senior Intelligence Official
SSO	Special Security Officer
SSR	Special Security Representative
TAG	The Adjutant General

### PART II. DEFINITIONS

Activity -- An entity consisting of National Guard Bureau Joint Staff Directorates at the Temple Army National Guard Readiness Center, Air National Guard Readiness Center, and National Guard Joint Directorates at the Pentagon.

Information Security -- The system of policies, procedures, and requirements established in accordance with reference k to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to Executive Order, statute, or regulation (reference b).

Open Storage Area -- Within the National Guard Bureau, an area constructed in accordance with the requirements of the appendix to Enclosure 3 of reference d and authorized by the senior agency official for open storage of classified information (reference d). Within the States, an area constructed in accordance with Title 32 Code of Federal Regulations, Part 2001, Section 2001.53, and reference n and authorized by the agency head for open storage of classified information. For the purposes of reference n, an open storage area also means an area that has been approved for open storage only to accommodate classified connectivity associated with, for example, the deployment of a classified information system.

Sensitive Compartmented Information -- Classified national intelligence information concerning, or derived from, intelligence sources, methods, or analytical processes that requires handling within formal access control systems established by the Director of National Intelligence. Also called sensitive compartmented information (reference a).

Special Security Representative -- An official who, under the supervision of Special Security Officers, performs the day-to-day management and implementation of the facility's sensitive compartmented information security program for subordinate sensitive compartmented information facilities.