



CHIEF NATIONAL GUARD BUREAU NOTICE

NGB-J2
DISTRIBUTION: A

CNGBN 2402
21 December 2017

NATIONAL GUARD INFORMATION SECURITY PROGRAM

References: See Enclosure A.

1. Purpose. This notice provides interim guidance for the National Guard (NG) Information Security (INFOSEC) Program in accordance with (IAW) references a through k.

2. Cancellation. None.

3. Applicability. This notice applies to all NG elements.

4. Background. The Department of Defense (DoD) INFOSEC Program is the foundation for the protection and management of all national security information IAW reference a. DoD implements this program IAW references b through k. The DoD Information Security Oversight Office (ISOO) establishes department standards for classifying and declassifying national security information, security education and training programs, safeguarding information, and self-inspection programs.

a. The Chief of the National Guard Bureau (CNGB) appointed a Senior Agency Official (SAO) and a Senior Intelligence Official (SIO) IAW reference b to assume responsibility for the safeguarding of collateral information and sensitive compartmented information (SCI), respectively.

b. The DoD ISOO issues an annual self-inspection checklist to all SAOs. The National Guard Bureau (NGB) SAO gathers INFOSEC program reports from each NG Joint Force Headquarters-State (NG JFHQs-State) Office and NGB Joint Staff (NGBJS) Directorate for submission to DoD ISOO, which ensures compliance and identifies areas for improvement. Failure to fulfill these responsibilities could result in the loss of NG access to DoD information and national security information systems.

UNCLASSIFIED

5. Action or Procedure. All NG members will properly protect classified information and Controlled Unclassified Information under their purview IAW references b through e. NG leaders in command, management, or supervisory positions will ensure the quality and effectiveness of the implementation and management of the NG INFOSEC Program within their areas of responsibility IAW references b through e. 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 Information Security Branch has developed training that meets these standards and is available for use by INFOSEC staff with responsibilities outlined in this notice. All NG INFOSEC training must comply with DoD standards by Fiscal Year 2018.

a. 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.

b. SIO. The SIO will coordinate with the NGB SAO as appropriate, to achieve a harmonized and cohesive NG INFOSEC Program.

c. Directors of the Army National Guard (DARNG) and 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 an ASM to properly manage and oversee that Service component's INFOSEC program IAW references b through e.

(2) Ensure compliance with the minimum requirements set forth in references b through e and establish a report channel, which includes the CNGB and SAO.

d. The Adjutants General (TAG). TAGs will appoint, at a minimum, one primary and one alternate Security Assistant to oversee their State's respective INFOSEC program IAW references b through e.

e. NG JFHQs-State. All NG JFHQs-State Offices will follow references b through e, as supplemented by CNGB Issuances, for the management and implementation of their programs.

f. ASM. The ASM will:

(1) Manage and implement the NG INFOSEC Program on behalf of the CNGB, DARNG, or DANG, respectively, to whom they will have direct access, IAW reference b.

(2) Ensure all activities, organizations, directorates, and offices under their security cognizance comply with the DoD ISOO annual self-inspection checklist reporting requirements.

(3) Appoint Security Assistants, as necessary.

g. Assistant ASM (AASM). AASMs will assist with program implementation, maintenance, and local oversight. AASMs must be United States citizens and possess the security clearance and access appropriate for their assigned responsibilities. AASMs report directly to their respective ASMs.

h. Security Assistants. Security Assistants will perform daily administrative security functions under the direction of the ASM or AASM to include:

- (1) Conducting initial and annual NG INFOSEC training.
- (2) Serving as the first line of defense against security incidents.
- (3) Gathering ISOO-related data and reporting it to the ASM.
- (4) Coordinating with other security leadership as needed.

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

7. Effective Date. This notice is effective on the date signed and will expire one year from the date of signature, unless canceled earlier.


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

Enclosure:

A -- References

ENCLOSURE A

REFERENCES

- a. DoD Instruction 5200.01, 21 April 2016, “DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)”
- b. DoD Manual 5200.01, Volume 1, 24 February 2012, “DoD Information Security Program: Overview, Classification, and Declassification”
- c. DoD Manual 5200.01, Volume 2, 24 February 2012, “DoD Information Security Program: Marking of Classified Information”
- d. DoD Manual 5200.01, Volume 3, 24 February 2012, “DoD Information Security Program: Protection of Classified Information”
- e. DoD Manual 5200.01, Volume 4, 24 February 2012, “DoD Information Security Program: Controlled Unclassified Information (CUI)”
- f. DoD Manual 5105.21, Volume 1, 19 October 2012, “Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security”
- g. DoD Directive 5205.07, 01 July 2010, “Special Access Program (SAP) Policy”
- h. Executive Order 13526, 29 December 2009, “Classified National Security Information”
- i. Executive Order 13556, 04 November 2010, “Controlled Unclassified Information”
- j. DoD Directive 5105.77, 30 October 2015, “National Guard Bureau (NGB)”
- k. CNGB Instruction 2200.01, 16 November 2015, “National Guard Access to Top Secret Sensitive Compartmented Information”