



CHIEF NATIONAL GUARD BUREAU INSTRUCTION

NG-J2
DISTRIBUTION: A

CNGBI 2200.01
16 November 2015

NATIONAL GUARD ACCESS TO TOP SECRET SENSITIVE COMPARTMENTED INFORMATION

References:

- a. DoD Directive 5105.77, 21 May 2008, “National Guard Bureau (NGB)”
- b. JP 2-0, 22 October 2013, “Joint Intelligence”
- c. DoD Directive 5105.83, 05 January 2011, “National Guard Joint Force Headquarters – State (NG JFHQs-State)”
- d. DoD Manual 5105.21, 19 October 2012, “Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security”

1. Purpose. This instruction establishes policy and assigns responsibilities for accessing Top Secret/Sensitive Compartmented Information (TS/SCI) containing critical threat information available only in a Sensitive Compartmented Information Facility (SCIF). This capability is a critical component of the National Guard Incident Awareness and Assessment (IAA), Defense Support of Civil Authorities (DSCA), Homeland Defense, and other domestic emergency missions, in accordance with (IAW) the references.

2. Cancellation. None.

3. Applicability. This instruction applies to all elements of the National Guard. States, Territories, and the District of Columbia, are hereafter referred to as “States.”

4. Policy. It is National Guard Bureau (NGB) policy that:

UNCLASSIFIED

a. The Chief of the National Guard Bureau (CNGB), The Adjutants General (TAG), the Commanding General of the District of Columbia National Guard (CG), and their designated staff have ready access to TS/SCI within one hour of notification.

b. If a SCIF is inaccessible within one hour of notification, a NG-JFHQs-State SCIF may be established either through minor construction or refit of an existing facility.

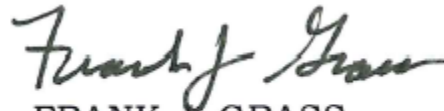
5. Definitions. See Glossary.

6. Responsibilities. See Enclosure A.

7. Summary of Changes. This is the first issuance of CNGBI 2200.01.

8. Releasability. This instruction is approved for public release; distribution is unlimited. Copies are available 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 within five years of its publication.



FRANK J. GRASS

General, USA

Chief, National Guard Bureau

Enclosures:

A -- Responsibilities

GL -- Glossary

ENCLOSURE A

RESPONSIBILITIES

1. CNGB. The CNGB will provide States with access to SCIFs, and critical threat information through information systems and programs, classified at the TS/SCI level in support of homeland defense.

2. Director of National Guard Joint Staff Directorate of Intelligence (NG-J2). The Director of NG-J2 will:

a. Implement guidance for managing the delivery of TS/SCI, critical threat information, to the States.

b. Collaborate with U.S. National Intelligence Agencies, IAW reference a.

c. Conduct and coordinate NG JFHQs-State capability assessments to identify specific TS/SCI capability shortfalls.

d. Publish guidance to the States on administering funding programs for establishing TS/SCI communication capabilities inside NG JFHQs-State.

e. Develop and execute annual program budget to develop TS/SCI capabilities in States lacking this capability, subject to availability of funds.

f. Submit funding shortfalls through the NGB's Unfunded Requirements (UFR) process.

g. Prioritize program funding for NG JFHQs-S TS/SCI capability shortfalls.

h. Seek funding solutions to prioritized funding shortfalls, IAW all applicable statutes and regulations.

3. Director of National Guard Joint Staff Domestic Operations and Force Development (NG-J3/7). The Director of NG-J3/7 will direct the flow of information to and from the States during National Guard DSCA and Homeland Defense missions.

4. Air National Guard Director of Intelligence (NGB/A2). The Director of NGB/A2 will:

a. Act as the proponent for Air National Guard (ANG) SCIFs.

b. Provide guidance to the States for the plan, design, construction and accreditation of ANG SCIFs.

c. Coordinate the accreditation process between the State J2's and the Defense Intelligence Agency (DIA).

5. Army National Guard Director of Intelligence and Security (ARNG-G2). The Director of ARNG-G2 will:

a. Act as the proponent for Army National Guard (ARNG) SCIFs.

b. Provide guidance to the States for the plan, design, construction and accreditation of ARNG SCIFs.

c. Coordinate the accreditation process between the State J2's and the DIA.

6. United States Property and Financial Officers (USPFO). USPFOs are accountable for the authorized use of program funding for all aspects of JFHQs-State SCIF's, IAW all applicable statutes and regulations. Funding for SCIFs is transferred to State USPFO offices for distribution.

7. TAG and the CG. TAGs and the CG will:

a. Establish State standard operating procedures (SOP) for accessing TS/SCI critical threat information.

b. Appoint a State Senior Intelligence Officer (SIO) and State Special Security Officer (SSO).

c. Appoint a single special security point of contact (POC) from the State for all special security aspects of establishing a JFHQs-S SCIF, to include planning, design, construction security, and the accreditation process.

8. JFHQ-S SCIF POC. The JFHQs-S SCIF POC will:

a. Conduct a comprehensive assessment of NG JFHQs-State TS/SCI capability requirements.

b. Coordinate funding with NG-J2 and other appropriate NGB elements.

c. Submit UFRs to appropriate elements, as required.

9. State SIO. The State SIO will, as needed:

a. Coordinate the accreditation process with the DIA through the ARNG-G2 or the NGB/A2.

b. Coordinate with NGB and other State and Federal agencies to obtain TS/SCI access at NG-JFHQs-State.

c. Request security clearances and administer access for TAG, the CG, and designated staff.

10. State Joint Operations Center (JOC). The State JOC will:

a. Maintain communications and situational awareness with the National Guard Coordination Center (NGCC).

b. Notify TAG, the CG, or designated staff of incoming critical threat information, as outlined in the State's SOP.

c. Confirm notification and receipt of incoming critical threat information by TAG, the CG, or designated staff.

11. SSO. Perform duties as outlined in reference d, and all other applicable issuances.

12. NGCC. The NGCC will:

a. Maintain communication and situational awareness with NG JFHQs-State JOCs.

b. Notify State JOCs of incoming critical threat information, as directed by NGB leadership and staff.

c. Confirm notification and receipt of incoming critical threat information to the NG-J3/7, within the prescribed one-hour time frame.

13. State Personnel Security Manager. The State Personnel Security Manager, in coordination with the State SSO, will process security clearances for TAG, the CG, and designated staff, IAW State, Service, and Federal guidance.

GLOSSARY

PART I. ACRONYMS

ANG	Air National Guard
NGB/A2	Air National Guard Directorate of Intelligence
ARNG	Army National Guard
ARNG-G2	Army National Guard Directorate of Intelligence and Security
CG	Commanding General of the District of Columbia, National Guard
CNGB	Chief of the National Guard Bureau
DIA	Defense Intelligence Agency
DSCA	Defense Support to Civil Authority
IAA	Incident Awareness and Assessment
IAW	In accordance with
JOC	Joint Operations Center
NGB	National Guard Bureau
NGCC	National Guard Coordination Center
NG-J2	National Guard Joint Staff Directorate of Intelligence
NG-J3/7	National Guard Joint Staff Directorate of Domestic Operations and Force Development
NG JFHQs-State	National Guard Joint Forces Headquarters-State
POC	Point of contact
TAG	The Adjutants General
SCIF	Sensitive Compartmented Information Facility
SIO	Senior Intelligence Officer
SOP	Standard operating procedures
SSO	Special Security Officer
TS/SCI	Top Secret/Sensitive Compartmented Information
UFR	Unfunded requirements
USPFO	United States Property and Fiscal Officer

PART II. DEFINITIONS

Access -- Formal indoctrination into a particular compartment of Sensitive Compartmented Information.

Accreditation -- The official management decision to permit operation of an information system in a specified environment at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

Sensitive Compartmented Information Facility -- A facility authorized and formally accredited by the Defense Intelligence Agency to process Sensitive Compartmented Information.