



# CHIEF NATIONAL GUARD BUREAU NOTICE

NG-J3/7  
DISTRIBUTION: A

CNGB Notice 3301  
07 June 2016

## NATIONAL GUARD CYBER THREAT WORKING GROUP

References: See Enclosure A.

1. Purpose. This notice provides interim guidance for the National Guard Bureau (NGB) Cyber Threat Working Group (CTWG) in accordance with references a through r.
2. Cancellation. None.
3. Applicability. This notice applies to all elements of the National Guard (NG) and will not conflict with pre-established Army National Guard (ARNG G6) and Air National Guard (NGB A2/3/6) communications for technical network operations. This notice is not intended to conflict with law, regulation, executive order, or directives.
4. Background. Cyber events frequently cross geographic and organizational boundaries. This necessitates a cross-functional team to evaluate events in order to effectively assess and communicate event details. The cross-functional team is formally defined as the CTWG. The CTWG established a process to create a unified strategic message from NGB staffs to the States, Territories and District of Columbia, to ensure the NG responds appropriately to cyber threats.
5. Action or Procedure.
  - a. Assessing, Communicating, and Responding to a Cyber Event. The Directorate of Domestic Operations and Force Development, Cyberspace Operations Division (NG-J36) will facilitate the CTWG with senior level representatives from the Directorate of Intelligence (NG-J2), the Law Enforcement and Mission Assurance Division (NG-J34), and the Directorate of Communications and Chief Information Officer (NG-J6/CIO). Participation varies depending on the risk assessment and may include representatives from the ARNG, ANG, Office of the NGB Chief Counsel, Office of the NGB Public

**UNCLASSIFIED**

Affairs (NGB-PA), Office of NGB Legislative Liaison (NGB-LL), other NG Joint Staff members, and impacted State representatives.

b. National Guard Coordination Center (NGCC) Role. The NGCC is the lead coordination element for the NGB. The Cyber Coordination Cell (CCC) supports the NGCC for cyber events. The CCC is led by the Chief of NG-J36 and integrates representatives from the NG-J2, NG-J34, and NG-J6/CIO. The CCC is a standing element that supports the Current Operations Division (NG-J33), maintains a steady-state presence as part of the NGCC, and integrates with the Adaptive Battle Staff (ABS) during major operations.

c. Initial Assessment. The NGCC conducts initial assessments of all-hazards events against the CNGB Critical Information Requirements (CCIRs). The NGCC gathers and evaluates information from all sources, including the States, Territories and District of Columbia reports, mission partners, and open sources to identify if potential cyber events require CTWG action. The NGCC will then use the CCC to assist in the initial assessment of the potential cyber events against CCIR criteria.

d. Convene the CTWG. If the CCC determines a cyber event exists, the CCC will convene the CTWG at the action officer level. Any CTWG member may convene the group based on the initial assessment of a cyber event. When this occurs, the convening member will immediately share the information with the NGCC. The CTWG may expand its membership, as required, to include additional action officers or O6 level members based on areas of impact and event severity to ensure all stakeholders are advised of the situation.

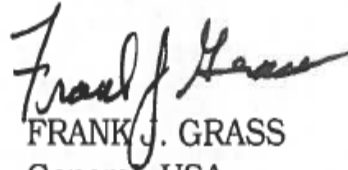
e. Situational Awareness Communication. The CCC and CTWG will provide support to the NGCC Team Chief by performing an initial assessment of the event, elevating to directorate level (if necessary), and notifying the CNGB concerning appropriate information sharing for the event and messaging.

f. Operational/Strategic Communication. The CCC and CTWG will identify events crossing multiple staffs, as well as events that require additional communications for purposes such as response, mitigation, or strategic messaging by NGB. For these events, the CTWG will identify and gather representation from all affected NGB staff elements, State, Territory and District of Columbia staffs, and when needed, mission partners. This group of stakeholders will develop recommended actions for NGB and identify a lead element to represent equities and ensure unified strategic messaging.

g. Link to Threat Working Group. The CTWG is linked to the Threat Working Group and both coordinate efforts between NGB staffs when supporting a national response or special event.

6. Releasability. This notice is approved for public release; distribution is unlimited. Copies are available 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.



FRANK J. GRASS  
General, USA

Chief, National Guard Bureau

Enclosure:

A -- References

ENCLOSURE A

REFERENCES

- a. DoD Directive 5105.77, 30 October 2015, “National Guard Bureau (NGB)”
- b. DoD Directive 3025.18, 21 September 2012, “Defense Support of Civil Authorities”
- c. DoD Instruction 5105.18, 10 July 2009, Incorporating Change 1, “DoD Intergovernmental and Intragovernmental Committee Management Program”
- d. 10 U.S.C. § 151, “Joint Chiefs of Staff: Composition; Functions”
- e. 10 U.S.C. § 10502, “Chief of the National Guard Bureau: Appointment; Advisor on National Guard Matters; Grade; Succession”
- f. Presidential Policy Directive 20 (PPD 20), 2012 (classified)
- g. JP 3-12, 05 February 2013, “Cyberspace Operations”
- h. JP 3-28, 31 July 2013, “Defense Support of Civil Authorities”
- i. CJCS Manual 6510.01B, 10 July 2012 “Cyber Incident Handling Program”
- j. CNGB Instruction 2000.01, 17 September 2012, “National Guard Intelligence Activities”
- k. CNGB Instruction 3301.01, 14 November 2013, “National Guard General Officer Advisory Council on National Guard Involvement in Cyberspace Activities”
- l. NGB Memo 380-16/33-361, 28 September 2010, “Personally Identifiable Information (PII) Incident Response Handling”
- m. Adaptive Battle Staff (ABS) Standard Operating Procedures
- n. National Guard Coordination Center Standard Operating Procedures, 20 February 2015
- o. NGB Cyber Coordination Cell Integration Plan, January 2015
- p. Army National Guard Computer Network Defense Team (CND-T) Concept of Operations, June 2015
- q. USCYBERCOM Cyber Force Concept of Operations & Employment (CFCOE), v4.1, 22 July 2014

r. USCYBERCOM Concept of Operations (CONOPS), 27 September 2010,  
“Chief Information Officer (CIO), Command, Control, Communications and  
Computers (C4) Systems and Architectures Annex, v1.0”