



DEPARTMENT OF THE ARMY
HEADQUARTERS, JOINT READINESS TRAINING CENTER AND FORT POLK
6661 WARRIOR TRAIL, BUILDING 350
FORT POLK, LOUISIANA 71459-5339

MAY 04 2016

AFZX-IM

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum G6-01 – Commander's Program to Manage Cybersecurity Risk

1. References.

- a. Memorandum, HQ FORSCOM, AFIT, 19 Dec 14, Policy Memo 14: Commander's Program to Manage Cybersecurity Risk.
- b. Fort Polk OPORD 13-108 - FRAGO 1-5, 10 Apr 13, subject: Commander's Program to Manage Cybersecurity Risk.
- c. Memorandum, HQ, Joint Readiness Training Center (JRTC) and Fort Polk, Command Policy Memorandum CG-01, Commander's Critical Information Requirements (CCIR).
- d. Army Regulation 25-2, Information Assurance, 23 Mar 09.

2. Purpose. To establish a commander's program that manages cyberspace risk through increased training, information assurance, greater situational awareness, and creating secure and resilient network environments.

3. Applicability. All Fort Polk units and installation activities.

4. Background. Leaders rely on cyberspace to enable mission command, training, force generation, logistics, and intelligence. Commanders must proactively protect and maintain freedom of maneuver within networks.

5. Policy.

a. Cybersecurity is a Commander's responsibility. We will hold leaders and individual users accountable for protecting information, networks, and the systems.

b. Commanders will establish a program to manage cyberspace risk. The program will include the following facets:

(1) Assessment. Units will continually assess their Cybersecurity posture. Commanders will develop a plan of action as well as assessment milestones utilizing the results from the information assurance self-assessment tool. Based on these assessments, commanders will determine how best to modify training and operating

AFZX-IM

SUBJECT: Command Policy Memorandum G6-01 – Commander's Program to Manage Cybersecurity Risk

procedures to maintain acceptable Cybersecurity posture. The self-assessment tool is to be completed NLT 15 Feb of every calendar year. The self-assessment tool is located at <https://iatraining.us.army.mil>.

(2) Training. Commanders will implement a formal Cybersecurity training program to ensure network users and Cybersecurity workforce understand their roles in keeping our networks secure. Commanders will ensure all users register in the Army Training and Certification Tracking System (ATCTS). The ATCTS tracks Department of Defense Cybersecurity training requirements which complement but do not replace the commander's assessment program. The ATCTS is located at the following link: <https://atc.us.army.mil/iastar/registration.php>.

(3) Security. Commanders will implement security directives for incident reporting and mitigation as outlined in the installation incident response plan. Commanders will verify effective security procedures are in place to protect information systems and data.

(4) Reporting. Commanders will report Cybersecurity incidents in accordance with Commander's critical information requirements as well as guidance outlined in the installation incident response plan.

(5) Accountability. Commanders are responsible for protecting our networks. Commanders will hold leaders and network users accountable for any activities that place our networks at risk. Commanders should consult with their legal office regarding financial liability (e.g., financial liability investigation for property or loss).

6. Any exception to this policy will be based upon urgent mission needs and requires the approval of the CG.

7. The point of contact for this policy is the ACoS G6 at commercial 337-531-1587 or DSN 863-1587.



GARY M. BRITO
Brigadier General, USA
Commanding

DISTRIBUTION:
A+

AFZX-IM
 SUBJECT: Command Policy Memorandum G6-01 – Commander’s Program to Manage
 Cybersecurity Risk

TAB A (UDCI Reporting Procedures)

