



REPLY TO  
ATTENTION OF:

**DEPARTMENT OF THE ARMY**  
HEADQUARTERS, 69TH AIR DEFENSE ARTILLERY BRIGADE  
32D ARMY AIR AND MISSILE DEFENSE COMMAND  
56012 TEDESCO WAY  
FORT HOOD, TEXAS 76544

AFVL-LBC

Date: 6 February 2014

**MEMORANDUM FOR RECORD**

**SUBJECT: Policy Letter #5, Cybersecurity Incident Withholding Policy**

**1. REFERENCES.**

- a. AR 380-5 (Department of the Army Information Security Program), 29 September 2000.
- b. AR 15-6 (Procedures for Investigating Officers and Boards of Officers), 2 October 2006.
- c. Memorandum, Secretary of the Army, 1 February 2013, subject: Mandatory Information Assurance/Cybersecurity Awareness.
- d. Army Regulation (AR) 25-2 (Information Assurance), 23 March 2009.
- e. FORSCOM EXORD (AFIN-SEC), 221916ZMAY12, Security Incident Reporting and Mitigation Guidance.
- f. AR 380-67 (Department of the Army Personnel Security Program), 4 August 2011.
- g. FRAGO 2, 5 February 2013, to U.S. Army Cyber Command EXORD 2013-276, Unauthorized Disclosure of Classified Information via Electronic Communication Reporting Procedures, 7 June 2012.
- h. FORSCOM Policy Memo 14, 4 March 2013, Commander's Program to Manage Cyberspace Risk.
- i. III Corps and Fort Hood Command Policy NEC-01, 2 November 2009, Computer Network Security.
- j. Rules for Courts-Martial 306(a) and 401, Manual for Courts-Martial (2012 Edition).
- k. AR 600-20 (Army Command Policy), 18 March 2008 (RAR 20 September 2012).
- l. III Corps and Fort Hood Regulation 27-10 (Military Justice), 10 November 2008.

AFVL-LBC

SUBJECT: Policy Letter #5, Cybersecurity Incident Withholding Policy

2. PURPOSE. To withhold authority to determine disposition of allegations of misconduct and/or disposition of charges and specifications over all incidents of cybersecurity incidents as defined in this policy letter.

3. APPLICABILITY. Headquarters, 69<sup>th</sup> Air Defense Artillery Brigade and all units assigned or attached.

4. DEFINITIONS.

a. A cybersecurity incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

b. Examples of cybersecurity incidents include, but are not limited to:

(1) Unauthorized disclosure of classified information (UDCI) or the synonymous common term "negligent discharge of classified information" (NDCI). UDCIs include, but are not limited to:

(a) Spillages: The introduction of classified information on a lower classified information system or a system with incompatible releasability restriction. Spillages must be contained and sanitized from every component of the Department of Defense (DoD) enterprise that may be infected.

(b) Loss of any information system equipment or media containing sensitive or classified information.

(2) Cross Domain Violation (CDV): The connection of a device and transfer of information on an information system that differs from its approved classification. CDVs typically occur when discipline is not properly enforced while moving a device connected to a DoD information system.

(3) Attempts to use or attach equipment and removable media (e.g. thumb drives, discs, etc.) not authorized for connection to DoD information systems. Such violations potentially introduce malware on a system.

(4) Attempts to access or collect data for which an individual is not cleared.

(5) Attempts to circumvent information system access controls designed to protect sensitive or classified information.

AFVL-LBC

SUBJECT: Policy Letter #5, Cybersecurity Incident Withholding Policy

5. POLICY.

a. I hereby withhold authority to determine the disposition of all cases concerning misconduct or alleged misconduct involving cybersecurity incidents. Subordinate commanders may request that I return the authority, on a case-by-case basis, to their level for disposition.

b. I will consider the full range of corrective actions at my disposal when cybersecurity incidents occur. Individuals responsible for cybersecurity incidents are subject to appropriate administrative, disciplinary, or criminal action. At a minimum, the account of the originating offender involved in the incident will be suspended while corrective action is pending, and a preliminary inquiry will be conducted IAW reference 1.a. when a suspected cybersecurity incident is discovered. A determination will be made if additional investigation is required IAW reference 1.b. For each violation, the offender will be required to take corrective training and recertification. Offender network access will not be restored until the above mentioned actions have been completed. Subsequent violations may require progressive correction actions.

c. Offender self-reporting is encouraged and may be considered as extenuation or mitigation if contemplating a disciplinary response to a cybersecurity incident.

6. REPORT. Unit commanders will report, through their chain of command, all instances of misconduct or alleged misconduct described in paragraph four of this policy letter to the Brigade Commander, Brigade Deputy Commander, Brigade Command Sergeant Major, Brigade S2, Brigade S6, and Brigade Judge Advocate within 24 hours of receipt of information.

7. Any exception to this policy will be based upon urgent mission needs and requires my approval.

8. This policy remains in effect until superseded or rescinded.

9. The point of contact for this policy letter is CPT Patrick Hurst, Brigade Judge Advocate, at 254-288-5944 or Patrick.j.hurst.mil@mail.mil



BRIAN W. GIBSON  
COL, AD  
Commanding