UNDER SECRETARY OF THE ARMY
WASHINGTON

10 MAY 2013

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Commander and Leader Responsibilities for Cybersecurity/Information Assurance (CS/IA) Incidents

1. References:

a. Army Regulation (AR) 25-2, Information Assurance, 23 March 2009.

b. AR 25-1, Army Knowledge Management and Information Technology, 4 December 2008.

c. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

d. AR 15-6, Procedures for Investigating Officers and Boards of Officers, 2 October 2006.

e. AR 380-67, Personnel Security Program, 4 August 2011.

f. AR 600-20, Army Command Policy, 20 September 2012.

2. Cybersecurity/Information Assurance (CS/IA) incidents cause unacceptable risks to national security and Army information systems, networks and data. They also significantly impact Army manpower, funds, equipment and operational capability. To prevent such incidents and enhance the Army's Cybersecurity posture, we must change Army culture. I therefore ask all Commanders and leaders to make a concerted effort to ensure organizational and individual accountability, proper and secure use of information systems, networks and data, greater Cybersecurity situational awareness, prompt recognition and mitigation of risks, and more training and awareness at all levels.

3. Commanders and leaders across the active Army, the Army National Guard and the U.S. Army Reserve are responsible for ensuring thorough reporting and enforcement of accountability for all suspected or confirmed CS/IA incidents. Such incidents are described in AR 25-2 and include but are not limited to: unauthorized disclosure of classified information and "spillage"; mishandling of classified or sensitive information (e.g., Personally Identifiable Information, Protected Health Information, For Official Use Only); loss of any information system or media containing classified or sensitive information; and other violations of CS/IA policies

or procedures.

4. Commanders and leaders will ensure that all suspected or confirmed CS/IA incidents are:

a. Responded to, investigated and reported in accordance with AR 25-2, AR 25-1, AR 380-5, other Army regulations relevant to the specific incident, Army Cyber Command procedures, and formal internal policies and procedures (e.g., Incident Response Plans, Continuity of Operations Plans).

b. Documented formally and reported throughout the appropriate chain of command, including to affected program managers, system owners, data owners, authorizing officials, designated approving authorities and original classification authorities.

c. Included in information system-related status briefings to senior leadership and throughout the chain of command.

d. Investigated in accordance with AR 15-6 upon suspicion or evidence of misconduct. Commanders will report credible derogatory information on personnel per AR 380-67.

e. Mitigated and resolved, with formal documentation of a plan to prevent a recurrence that addresses the root cause and contributing factors.

5. Commanders and leaders will hold all Soldiers, civilians, contractors and any other individuals accessing Army information systems, networks or data accountable for any actions or lack thereof that result in a CS/IA incident. When appropriate, sanctions will be imposed and can be increased for repeat offenses.

6. The point of contact for this issue is Mr. LeRoy Lundgren, Deputy Director, CIO/G-6 Cybersecurity Directorate: (703) 545-1679 or leroy.lundgren.civ@mail.mil.

Joseph W. Westphal

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
(CONT)

DISTRIBUTION: (CONT)
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Pacific
U.S. Army Europe
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Africa
U.S. Army Cyber Command
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Forces Strategic Command
U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Criminal Investigation Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Installation Management Command
Superintendent, United States Military Academy
Director, U.S. Army Acquisition Support Center

CF:
Director, Army National Guard
Director of Business Transformation