DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer/G-6

SAIS-CB

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Data Spillage and Unauthorized Disclosure Policy

1. References: See Enclosure 1.

2. Purpose. This memorandum and its enclosures clarify and reinforce Army policy associated with suspected or confirmed cybersecurity/information assurance (CS/IA) incidents of data spillage, unauthorized disclosure of unclassified sensitive information/controlled unclassified information (CUI), unauthorized disclosure of classified information (UDCI), negligent discharge of classified information (NDCI) and classified message incidents (CMI). These incidents are hereinafter referred to as CS/IA incidents.

3. Applicability. The policy in this memorandum and its enclosures applies to the active Army, the Army National Guard/Army National Guard of the United States and the U.S. Army Reserve. Personnel subject to this policy include, but are not limited to: Army civilian employees; Army contractors; employees of Army contractors; active, Reserve, and National Guard military members; and, as permitted by law and higher policy, authorized users of Army systems, networks, information and data. This memorandum does not assign or change responsibilities.

4. Policy.

a. General Policy.

(1) Any personnel who willfully or negligently cause a data spill or unauthorized disclosure may be subject to appropriate administrative, judicial, contractual or other disciplinary/corrective actions; and may additionally be subject to civil and/or criminal penalties in accordance with applicable regulations and law.

(2) Personnel discovering potential classified or unclassified sensitive information/CUI that is not otherwise properly protected or safeguarded must immediately execute all of the following actions: take physical custody of any loose material; safeguard any loose material; or electronic data and begin initial notification per Enclosure 3 of this memorandum. Personnel must not confirm or deny to any

unauthorized personnel or members of the public any knowledge or suspicion that the information is classified or sensitive unclassified information/CUI.

(3) All suspected or confirmed CS/IA incidents will be responded to, investigated, and reported in accordace with this memorandum, its enclosures and the latest versions of: Army Regulation (AR) 25-2; AR 380-5; other Army regulations relevant to the specific incident; Army Cyber Command (ARCYBER) and Second Army procedures; IA best business practices (e.g., references i and j); formal internal policies and procedures (e.g., incident response plans, continuity of operations plans); and any amplifying protection and handling guidance required by law or federal regulation.

b. See Enclosure 2 for terms, responsibilities and prevention.

c. See Enclosure 3 for initial notification and public disclosure.

d. See Enclosure 4 for immediate actions, reporting and record keeping.

e. See Enclosure 5 for categorization and investigations.

f. See Enclosure 6 for remediation, mitigation, cost determination and reimbursement.

5. This memorandum and its enclosures will be effective immediately upon signature, will remain in effect until rescinded and will be reviewed for update annually. The point of contact for this memorandum is Ms. Melissa Hicks, CIO/G-6 Cybersecurity Directorate: melissa.c.hicks.civ@mail.mil or (703) 545-1604.

FERRELL.ROBERT.SILAS.1028607268

Digitally signed by FERRELL.ROBERT.SILAS.1028607268
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=FERRELL.ROBERT.SILAS.1028607268
Date: 2016.05.02 08:19:33 -04'00'

Encls

ROBERT S. FERRELL
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
- U.S. Army Forces Command
- 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/Southern European Task Force
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- 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
Executive Director, Arlington National Cemetery
Commander, U.S. Army Accessions Support Brigade
Commandant, U.S. Army War College
Commander, Second Army

CF:
Director, Army National Guard
Director of Business Transformation
Commander, Eighth Army
Commander, U.S. Army Cyber Command