U.S. ARMY CHEMICAL MATERIALS AGENCY
5183 BLACKHAWK ROAD
ABERDEEN PROVING GROUND, MARYLAND 21010-5424

REPLY TO
ATTENTION OF:

AMSCM-D

31 AUG 2005

MEMORANDUM FOR All US Army Chemical Materials Agency Employees

SUBJECT: US Army Chemical Materials Agency Operations Security (OPSEC) Policy for Information to be Released to the Public

1 References:

a. Message, Department of the Army, DAMO-AOC, 141637Z Feb 05, subject: (U) Vice Chief of Staff of the Army (VCSA) Sends – Sensitive Photos.

b. Electronic Mail, US Army Materiel Command (AMC), 02 Aug 05, subject: CG Sends – OPSEC (Enclosure).

c. Message, Department of the Army, DAMO-AOC, 200001Z Aug 05, subject: (U) Chief of Staff of the Army (CSA) Sends -- OPSEC Guidance.

d. Army Regulation (AR) 530-1, OPSEC, 3 Mar 95.

2. References a, b, and c contain CSA, Commander, AMC, and VCSA guidance on OPSEC responsibilities. Reference d contains procedures to follow in conducting an OPSEC review.

3. In accordance with references a, b, and c, OPSEC is a chain of command responsibility and of particular concern is the posting of sensitive information and photographs to the internet, as well as specific categories of information identified by the AMC Commander (enclosed). OPSEC violations needlessly place lives at risk and degrade the effectiveness of operations.

4. Effective immediately within the US Army Chemical Materials Agency, the following policy is in effect. In accordance with procedures in paragraph 4-2, AR 530-1, all information (visual, electronic, hardcopy, or information by other visual/electronic means, including memoranda, letters, news releases, briefings, photographs, drawings and videos, or other visual or electronic information) that is to be released to the public will be given an OPSEC review by the installation or activity OPSEC Officer prior to release.

AMSCM-D 31 AUG 2005

SUBJECT: US Army Chemical Materials Agency Operations Security (OPSEC) Policy for Information to be Released to the Public

5. The staff proponent for this policy is the CMA Security Office, AMSCM-OPOC, 410-436-4431/6918.

Encl

MICHAEL A. PARKER
Director

From: Wentz, Paul L. COL AMCCG
Sent: Tuesday, August 02, 2005 2:17 PM
To: Hack, Richard LTG AMCDCG; Szymanski, Kathryn SES; Viall, Maureen AMC G1; Chaney, Anthony W. COL; Stevenson, Mitchell... MG. AMCOPS/G3; Baker, Sue AMCOPS G3; Mizusawa, Bert; Motsek, Gary SES G3; Finegan, Janis AMCPC/G5; Buckner, James D. SES G8; Leiby, Barbara SES AMC G8; Parsons, Jeffrey SES AMCCP; Darius, Bob AMCHO G1; Moon, Steven COL; Powell, Daryl; McCoy, Susan AMCIR; Parise, Robert J SES AMCCC; Napier, Thomas Z. COL AMCIG; Ashley, Lew; Crosson, Scott AMCSB CG; 'johnsonj@iadc-rock4.army.smil.mil'; 'radinr@iadc-rock4.army.smil.mil'; 'james.pillsbury@redstone.army.smil.mil'; 'lenaersw@KSYKNR04.army.smil.mil'; Hackett, Craig MG USASAC; 'michael.parker@apgea.army.smil.mil'; 'andersonc@riyadh.army.smil.mil'; Nadeau, Roger A., BG; Mazzucchi, Michael R MG CG C-E LCMC/PEO; Bolander, Brent T. LTC AMCSGS
Cc: Richardson, Thomas COL AMCDCG; Lunasco, Dave AMCCS; Kachinski, Kevin LTC AMCCG; Cockerham, K. Gary MAJ. AMCCG; Hewitt, Jyuji AMCDCG; Newman, Tom COL. AMCCG-SG; Ferrari, John LTC
Subject: CG Sends--OPSEC
Importance: High

Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Ladies and Gentlemen,
The Commanding General directed me to forward the following memo that addresses his concerns for OPSEC and the need for all to be more sensitive to what information we pass over unclassified means and when responding to press or other requests for information....

V/R,
COL Wentz

Ladies and Gentlemen,

AMC soldiers, civilians and contractors are doing a great job supporting the defense of our nation and are making tremendous strides in the process. However, in our eagerness to share these great accomplishments, we must remember to keep OPSEC in the forefront. Recent incidents should remind all of us that the current security environment poses serious threats to AMC and to our military as a whole, at home as well as abroad. We must all ensure that we are doing everything possible to protect the lives of our soldiers and their families; and ultimately to not put our soldiers; DA civilians, and contractors at risk through inadvertent disclosure of classified or sensitive information.

As the global war on terrorism continues, it is becoming increasingly important that we continue our efforts to protect operationally significant information that identifies our operational plans and vulnerabilities. In this global war, we face a stealthier enemy; information is everything and is the single determinant of advantage. We do not want to create a situation whereby our adversaries can use our own information to deter or defeat our mission, compromise our operations, or lead to friendly and allied deaths or casualties.

The enemy has continuously shown a capability of gathering open source information on Army operations, equipment and personnel. We must exercise caution when determining what information will be released to the public or posted to our public web sites. Each command must have an OPSEC review process in place. The review should include a series of local reviews by specific organizations and staff elements, to include the G2, OPSEC point of contact and the Public Affairs Office (PAO). These OPSEC reviews are designed to serve as a safeguard to eliminate

inadvertent and unauthorized disclosures of sensitive information to reduce our OPSEC vulnerabilities.

All personnel involved with originating information intended for public release (documents, seminar briefings, technical papers for publication, video tapes, CD ROMs, web site material, newsletters, interviews with the media), must be aware of and become familiar with this process within your commands.

Below you will find examples of potentially inappropriate information for public release:

-Equipment capabilities, limitations, vulnerabilities.
-Readiness and vulnerability assessments.
-Test locations and dates.
-Sensitive unclassified reports for internal Army use.
-Technical and scientific proprietary data developed by a contractor.
-Unclassified technical data with military applications.
-Lessons learned that could reveal sensitive military operations, exercises, or vulnerabilities.
-Movement of assets where uncertainty of location is a program or operational element.
-Logistics support (munitions, weapons movement).
-Specific, real-time support to current/ongoing military operations.

The Army cannot function without your efforts. Protecting our information is vital if success is to be achieved in carrying out the Army's missions. In order to accomplish such an endeavor, I call upon all AMC leaders, employees, contractors, and tenants to integrate OPSEC considerations into your daily operations. In addition, we need to ensure that all regulatory and local OPSEC policies and procedures are being earnestly and properly followed. We owe this to those in harm's way!

BENJAMIN S. GRIFFIN
General, USA
Commanding

Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Steve A. Cowan — Steve A. Cowan — 08 SEPT 05
Rollie Robinson — Rollie Robinson — 8 Sept 05
Christopher T. Chester — Christopher T. Chester — 8 Sept 05
Carol Hunter — Carol Hunter
8/29/2005 — Donald VanWinkle — Donald VanWinkle — 12 Sept 05
12 Sept 05