United States Army
Criminal Investigation Command

Media contact: CID Public Affairs Office
571-305-4041

FOR IMMEDIATE RELEASE

CID Lookout
On Point for the Army

CID Cyber Tips:

Protecting Your Online Identity

QUANTICO, Virginia, September 13, 2013 – Now more than ever, Soldiers, Army civilians, and family members rely on the Internet to work, study, stay connected with family and friends, pay their bills or simply unwind. For criminals, the Internet provides an endless stream of potential targets to be victimized.

The U.S. Army Criminal Investigation Command, commonly known as CID, continually receives various reports ranging from identity theft to Internet scams, perpetrated by cyber criminals operating throughout the world. Law enforcement's ability to identify these perpetrators is difficult and limited, so individuals must stay on the alert and be personally responsible for their online presence to protect both themselves and their loved ones.

As such, CID is providing the following information to help the greater Army community protect themselves online and significantly reduce the chance of becoming a victim of cyber crime.

How to protect yourself:

ONLINE

- **Know the terms on social networking websites.** Facebook, Twitter, LinkedIn and other social networking sites privacy settings default to ***everyone***. This means ***anyone,*** can view your profile, not just people you know. Users can and should change this by accessing the Privacy Settings/Profile Information usually found under the respective Account tab.

- **Sample social networking safely.** Never disclose private information when using social networking websites. Be very selective about who you invite or accept invitations from as cyber criminals use false profiles to gain access to personal and private information, such as birthdates, marital status, and personal photographs. Posts containing personal identifying information (PII), including pictures containing metadata can be used against you and your family.

- **Click with caution.** Always use caution when clicking on links in an email or a social networking post, even from someone you know. Reports of personal social networking accounts being hacked and taken over by criminals have increased in recent years. Clicking on a link that appears to be benign in nature may in fact contain embedded malware that can compromise your computer. Once compromised, the data on your computer can be exploited and even your computer can be remotely operated as a surrogate in online attacks against others.

- **Hide your profile from search engines**. This can be accomplished by going to the Account/Privacy Settings/ Search and unchecking the "Public Search Results" box. This will remove your public preview from Google, Bing, and Yahoo search returns.

- **Prevent people from "tagging" you in photos and videos.** To do this, go to the Account/Privacy Settings/Profile Information/Photos and Videos of Me and deselect the ***everyone*** default.

- **Keep your personal information safe.** Don't provide personal or financial information, user names, or passwords in response to an email, because legitimate companies generally don't seek such information in this manner.

- **Install/update your anti-virus/firewall software.** Antivirus and firewall software is a must for anyone to safely navigate online. Always keep your security software up to date in order to provide the most complete protection from malicious programs as thousands of new viruses are detected every year. Also, ensure your antivirus software program updates automatically and scans your computer on a recurring schedule.

- **Free antivirus support from ACERT.** Current Department of Defense employees (excluding contractors, retirees, and family members) with an active AKO account can download antivirus software for free by logging in to the United States Army Computer Emergency Response Team website and selecting the Antivirus link.

SMARTPHONES/MOBILE DEVICES

- **Know your Apps.** When signing up with an app store or downloading individual apps, you may be asked for permission to let them access information on your device. Some apps may be able to access your phone and email contacts, call logs,

Internet data, calendar data, data about the device's location, the device's unique ID, and information about how you use the app itself. If you're providing information when you're using the device, someone may be collecting it.

- **Passwords protect all devices.** The time to safeguard the information on your portable electronic device is not after it has been lost or stolen. Ensure all portable electronic devices are properly password protected, especially any device with personal communications account information (email, Facebook, Twitter, LinkedIn, etc.).

- **"Brick" a stolen device.** In recent years, roughly 40% of all robberies now involve smart phones and/or tablet computers (iPad, Kindle Fire, etc.). Thus endangering the security of the personal information on the stolen devices. If a person's smart phone is lost or stolen, they may now contact the carrier and ask to have that device remotely disabled. These **"Bricked"** phones are of little or no use to thieves because they can't be reactivated after being sold on the black market.

Where to go for help:

If you are a **victim** of an online scam where the likeness of a U.S. Soldier was utilized (false social media/dating profiles, photographs, etc.) with **no further Personally Identifiable Information disclosed**, the following actions should be completed as soon as possible to assist law enforcement:

Report the theft to the Internet Crime Complaint Center (IC3) (FBI-NW3C Partnership). Online: http://www.ic3.gov/default.aspx

If you suspect you are a victim of identity theft, you should report the crime to the **FBI IC3**, as well as report the theft to the **Federal Trade Commission**. Your report helps law enforcement officials across the United States in their investigations.

Online: http://www.ftc.gov/idtheft

By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261

By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

CID strongly recommends that Soldiers, civilians and family members who have information of any known crime committed by a Soldier or a crime that occurred on their respective post, camp or station to report the incident to their local CID office or email CID at Army.CID.Crime.Tips@mail.mil.

-30-

CID Lookout is a U.S. Army Criminal Investigation Command (USACIDC) initiative to partner with the Army

community by providing a conduit for members of the Army family, to help prevent, reduce and report felony-level crime.

The USACIDC, commonly known as CID, is an independent criminal investigative organization that investigates serious, felony-level crime such as murder, rape, sexual assault, robbery, arson, fraud, and even cyber crime or intrusions into the Army networks (see CID Cyber Lookout).

Solving and preventing these types of crime cannot be achieved solely by CID Special Agents and the Military Police. Together, professional law enforcement officers and the Army community must work hand-in-hand to fight serious crime. As such, CID is *On Point for the Army* and depends heavily on Soldiers, family members and civilian employees to *Be On The Lookout* and provide assistance in keeping the *Army Strong* and safe.

CID Lookout provides the latest information to the Army community aimed at helping Soldiers protect themselves, their families and to reduce their chances of becoming crime victims.

For more information on CID or to report a felony-level crime or provide information concerning a crime, contact your local CID Office or the Military Police, or visit www.cid.army.mil.

-30-