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

Social Network Safety:

How to Protect Your Identity Online

QUANTICO, Virginia, December 11, 2014 – As a result of recent world events and a continual effort to protect the force, special agents with the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU) are strongly recommending that anyone affiliated with the U.S. military, review their social media accounts to make sure they are using the best security settings to protect their online profiles.

Social media platforms such as Facebook, Twitter and LinkedIn are powerful tools that can help bring communities together. However, an individual's online profile can provide cyber criminals with an endless pool of personal information and potential targets to be exploited. As such, it is vital that individuals stay on the alert and be personally responsible for their online presence to protect themselves, their loved ones and the Army.

With that in mind, 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.

Social Networking Safety Tips:

THINGS TO KNOW

- **The internet does not forget.** Once something is posted on a social networking website it can spread quickly, and no amount of effort can delete it. Do not post anything you would be embarrassed to see on the evening news.

-more-

- **You are not anonymous.** Cyber criminals have the capability to gather and exploit both individuals and organizations if the information is out there.

- **More isn't always better.** Participating in multiple social networking sites significantly increases ones risk and affords cyber criminal alternate avenues to strike and gather information.

HOW TO PROTECT YOURSELF:

- **Know the terms on social networking websites.** Facebook, Twitter, LinkedIn and other social networking sites frequently change their privacy and user policies. Social Networking sites privacy settings default to ***everyone***. This means ***anyone,*** can view your profile, not just the people you know. Securely configuring ones account will minimize who can see your information.

- **Safe social networking.** Never disclose private information when using social networking websites. Be very selective who you invite or accept invitations from as criminals often use false or spoofed profiles to gain access to personal and private information, such as birthdates, marital status, and photographs. Social media posts that contain personal identifying information (PII), digital photos that contain metadata (i.e., information written into the digital photo file such as who owns it, contact information, location, and internet search terms) can be used against you and your family.

- **Click with caution.** Always use caution when clicking on links in social networking posts, even from someone you know. Reports of personal social networking accounts being hacked 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 device. Once compromised, any data on your device can be exploited.

- **Hide your profile from search engines**. This can be accomplished by going to the social networking site account settings and unchecking the "Public Search Results" box. This will remove your public preview from Google, Bing, and Yahoo search returns.

- **Check-out and tag-out.** Do not use check-ins or post your specific location on social media. Also, prevent people from "tagging" you in photos and videos***.***

- **Login No No's.** Do not use your social networking site to login to other sites or use the save password, remember me, and keep me logged in options from a public or shared device. Use strong, unique passwords and never use the same password for all online accounts.

- **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.

As a service to the U.S. Army and DoD communities, CCIU has produced comprehensive how-to guides to safely configure an individual's Facebook and Twitter accounts. Configuration guides for other social networking platforms will be available in the near future. To download the guide visit http://www.cid.army.mil/documents/CCIU/2can/SocialNetworkingSafetyTips.pdf and select the respective guide at the bottom of page one.

Additional information about computer safety and cyber related crimes can be found on the U.S. Army Criminal Investigation Command's CCIU webpage at http://www.cid.army.mil/cciu.html. Simply select the Cyber Crimes Advisories on the left side of the page to review previous cyber crime alert notices and prevention flyers.

CID strongly recommends that Soldiers, civilians and family members who have information of any known crime committed by a Soldier, a crime that occurred on their respective post, camp or station, or is a victim of a crime to contact their local CID office, dial 1-844-ARMY-CID (844-276-9243) 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.

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.