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

Caution When Using myPay or No Pay Apps

QUANTICO, Virginia, October 18, 2013 – The U.S. Army Criminal Investigation Command, commonly referred to as CID, is warning the greater Army community about the potential dangers of using non-DOD sanctioned applications to access Defense Finance Accounting Services (DFAS) accounts.

On July 13, 2013, the free mobile application "MyPay DFAS LES" was released on the Google Play Android App store. Google estimates that between 10,000 to 50,000 individuals have already downloaded and installed this App on their personal mobile device. The App purportedly allows users the ability to control their individual military pay account after they enter their myPay login information.

In addition to this App, there are several other third party non-DOD sanctioned mobile applications available for Android and iPhone devices designed around DFAS payment processes for DOD military and civilian personnel, retirees and annuitants, as well as other government agencies.

CID is cautioning that using non-DOD sanctioned applications to access myPay accounts can potentially lead to one's personal account information being compromised and possibly the theft of funds.

Tips to help protect yourself:

- Before downloading, installing, or using an application, take a moment to research and review the software developer. This helps in getting an idea about other Apps the developer has previously published.

-more-

- Apps that imply to **allow access to military or government sites** should only be installed if they are **official** Apps sponsored by the DOD or another U.S. Government agency.

- Review the user ratings and reviews from previous and current customers as to the accuracy of the application's claims.

- Inspect your devices' application permissions screen to see what other information and applications will be accessed by the App. 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.

For more information regarding cyber crime and staying safe online, visit the CID Lookout or the Computer Crimes Investigative Unit webpage page at www.cid.army.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.