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 warns of posting holiday travel plans on the internet

Quantico, Va., Dec. 7, 2015 – As Soldiers and their families prepare for the holiday season, the U.S. Army Criminal Investigation Command, commonly referred to as CID, warns that posting travel plans on social media sites makes your home vulnerable to burglary.

While Soldiers should always be vigilant in their postings to avoid releasing sensitive information, revealing personal holiday travel information puts Soldiers, their families and their homes at risk.

“Social media is a powerful and frequently used tool for Soldiers, their families, and friends to stay connected, especially during the holiday season," Daniel Andrews, director of the CID’s Computer Crime Investigative Unit, said. "Unfortunately, criminals use the same social media sites to conduct surveillance and identify potential targets.”

In fact, Andrews said, posting vacation plans is like announcing to criminals that your residence will be unoccupied for an extended period.

“We recommend that personnel avoid publicizing the details of holiday plans and travel arrangements, whether upcoming or in progress,” Andrews said. “Wait until the vacation is over to comment on it and share photos, but still be cautious about what information you make publicly available.”

Additionally, personnel are advised to take basic home security measures before leaving their house.

The FBI’s “2014 Crime in the United States” reported an estimated 1,729,806 burglaries in the U.S., with burglaries of residential properties accounting for 73.2 percent. The average dollar loss for each burglary incident was $2,251.

Basic home security measures, such as locking all doors and windows, not leaving spare keys outside, using variable light timers, keeping valuables out of sight, and having a friend retrieve mail and newspapers are the first line of defense against burglary.

The use of a home security or video system is a further deterrent for criminals.

“Criminals are always on the lookout for opportunities to exploit. Whether driving through neighborhood streets or surfing social media sites, the criminal's goal is to identify ‘soft targets’ that are lucrative and present the least chance of being caught,” Andrews said. “This underscores the very real connection between the physical and virtual worlds.”

CID officials encourage Army personnel to take the following steps to reduce their risk of being targeted by crooks in the virtual world:

- Update your privacy setting on social media sites before leaving for vacation.
- Do not “check in” to airports or your holiday destination on social media sites. Sites, such as Facebook, use the GPS built into a phone to allow users to “check in” to businesses and locations across the country. This information tells would-be burglars that the home is likely to be vacant until the user announces their arrival at the airport for their return flight.
- Do not post in “real-time.” Posting information about your location while you are there is equivalent to telling a would-be burglar that you are not home. To minimize the risk of burglary while you are away, post information after you return home for the holidays.
- Remove GPS data from pictures. GPS data, to include location coordinates, is automatically attached to photos taken from both smart phones and many digital cameras. When posted in real-time, the GPS coordinates gives a would-be burglar your exact location, which makes your home vulnerable if you are not there.
- Do not geotag posts or tweets. Much like the Facebook “check in” feature, geotagging or adding your exact GPS coordinates to a Tweet or post tells would-be burglars exactly how close you are to your home.
- Monitor what family members post. A would-be burglar only needs one member of the family to announce that the family has left for vacation to know the house might be empty. Speak to all members of the family, especially teens, about what they are posting online.

Additionally, personnel should review CID’s Computer Crime Investigative Unit’s crime prevention and online safety flyers at www.cid.army.mil/cciu2can.html for more ways to avoid being victimized.

-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 cybercrime 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.