# eGuardian:
# Threat and Suspicious-Activity Reporting

*"Whether a plan for a terrorist attack is homegrown or originates overseas, important knowledge that may forewarn of a future attack may be derived from information gathered by state, local, and tribal government personnel in the course of routine law enforcement and other activities."*

*—National Strategy for Information Sharing*[1]

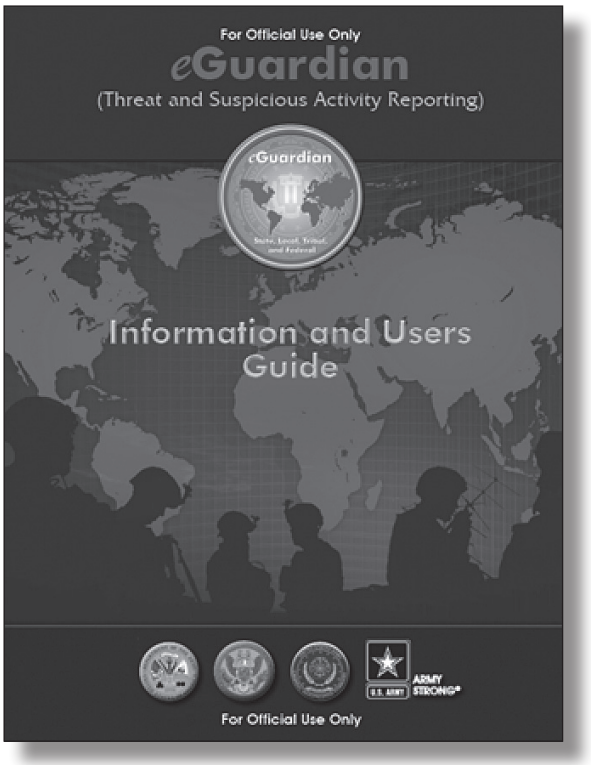
Department of Defense Instruction (DODI) 2000.26, *Suspicious Activity Reporting*,[2] directs the Department of Defense (DOD) to use the eGuardian system as the authorized law enforcement suspicious-activity[3] reporting system. eGuardian—developed, owned, and operated by the Federal Bureau of Investigation (FBI)—is a sensitive, unclassified reporting system; and access is restricted to law enforcement personnel and analysts. The system—

- Allows the FBI to collect suspicious-activity threat information that has a potential link to terrorism.
- Migrates threat information to the internal Guardian system, where it is assigned to the appropriate joint terrorism task force for further investigative action.
- Shares threat information with other federal law enforcement agencies as well as state, local, and tribal law enforcement agencies.

The FBI created eGuardian in 2008 to report and share potential unclassified terrorist threats, events, and suspicious activity among law enforcement agencies, fusion centers, and terrorism task forces. Information received via eGuardian is reviewed and analyzed at all levels to identify current threats, emerging trends, and future indicators. Although some suspicious-activity reports may not clearly indicate terrorism, the information is retained for 5 years and can be used for pattern and trend analysis. Incidents determined to have "no link to terrorism" are removed from eGuardian within 180 days of the final determination.

To strengthen efforts to counter terrorist threats, those responsible for protecting DOD resources must have timely access to properly acquired threat information. This includes information on terrorists' plans, capabilities, activities, and intended targets.

eGuardian plays a critical role in the ability to fight terrorists by reporting suspicious activity and assisting criminal intelligence analysts in their efforts to assess and warn the Army community of credible threats. It helps commanders determine the aggregate threat and keeps them informed of threat conditions, which allows them to initiate effective security responses and threat countermeasures. Remember, the ability to detect, report, and deter threats is as important as our ability to respond to them!




**eGuardian Information and Users Guide**


**eGuardian poster**

The management, oversight, and control of eGuardian within most of the Army[4] rests with the Office of the Provost Marshal General, which delegated program management to the U.S. Army Criminal Investigation Command (commonly referred to as "CID"). The Army's military intelligence community and Army subordinate commands (down to installation, unit, and facility level) are responsible for establishing education and reporting procedures that contribute to the timeliness and quality of suspicious-activity reporting. Within the Army Protection Program, threat working groups must work closely with their supporting CID office, provost marshal, or directorate of emergency services to establish a system to receive timely threat information.


**Law Enforcement Online seal**

Although eGuardian is in the early stages of Army-wide implementation, enhanced education and suspicious-activity awareness have led to an increase in suspicious-activity reporting. And suspicious-activity awareness campaigns and Army leader education will further increase reporting, which will result in greater situational awareness and enhanced analysis.

DOD personnel whose law enforcement responsibilities require access to eGuardian must establish Law Enforcement Online accounts at <*http://www.leo.gov*>. There are four account types approved for use by DOD personnel: user, supervisor, approver, and read-only.

For more information about eGuardian or to download products for local distribution, visit the Office of the Provost Marshal General Antiterrorism Enterprise Portal on Army Knowledge Online at <*https://www.us.army.mil/suite/page/605757*>. In the Antiterrorism Awareness ToolKit section, you will find an eGuardian Information and User's Guide, an information poster, and a suspicious-activity categories pocket card.

**Endnotes:**

[1]National Strategy for Information Sharing, October 2007, <*http://georgewbush-whitehouse.archives.gov/nsc/infosharing/sectionIV.html*>, accessed on 26 January 2012.

[2]DODI 2000.26, *Suspicious Activity Reporting*, 1 November 2011.

[3]"Suspicious activity," as defined by the FBI, refers to observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism or criminal or other illicit intention. Suspicious activities may include surveillance, cyber attacks, probing of security, and photographing of key infrastructure facilities.

[4]eGuardian within the National Guard is managed by the National Guard Bureau Provost Marshal.

*This article was written by staff from the Antiterrorism Branch, Office of the Provost Marshal General; the Law Enforcement Branch, Office of the Provost Marshal General; and CID.*