



Counterterrorism Division National Threat Center Section

January 16, 2009

eGuardian Threat Tracking System

Background: The **Guardian** Program was developed by FBI's Counterterrorism Division to communicate reports about suspicious activities that may be linked to terrorism, standardize the basis for such reporting, and enable further review in an organized and timely manner to determine if additional investigative follow-up is warranted by the law enforcement (LE) community. The **eGuardian** system extends capabilities currently housed in the **SECRET** Guardian system for regional and federal partners to state, local, and tribal (SLT) law enforcement partners at the **UNCLASSIFIED** level by hosting the application on a secure but unclassified Internet network administered by Law Enforcement Online (LEO). Inclusion of standardized processes at each layer within the workflow architecture facilitates quick but appropriate movement of information throughout the law enforcement system.

System Overview: The eGuardian system is intended to function as an alert, recording and reporting system for law enforcement. It allows recognized LE entities to record suspicious activity or threat information with a potential nexus to terrorism, in a standardized format using pre-defined business process flow, and submit the information for review and analysis at the local agency and regional levels.

"Suspicious activity" is defined as observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or illicit intention – a definition consistent with that utilized by the Program Manager/ Information Sharing Environment (PM/ISE).

Information is ingested into the system to assist in assessing terrorism-related threats and suspicious activities, enabling analysis of links, relationships, and matches among data elements. Tools included in eGuardian will enable analysts and investigators to quickly develop leads, identify potential suspects, and share vetted information with LE at all levels of government. At any point, information may be appended or linked to these incident reports using tools incorporated into the eGuardian and Guardian systems.

Access to eGuardian is through a Special Interest Group (SIG) hosted via LEO. Once validated, accounts can be accessed from any computer with Internet access. Information that first appears to be suspicious may turn out, upon further vetting, to be innocuous. Some information that is entered into eGuardian may reflect potential criminal conduct, but not conduct that amounts to terrorism. Furthermore, investigation and vetting of that information will necessarily be overly broad and contain personal information. Concerns about inappropriate sharing of personally identifiable information are mitigated by inclusion of customizable workflow and accesses based on each agency's own requirements; federal, state and local criteria for data retention; and data segmentation. Access to eGuardian is based on role and function: users must be sworn law enforcement officers or support personnel assigned to perform law

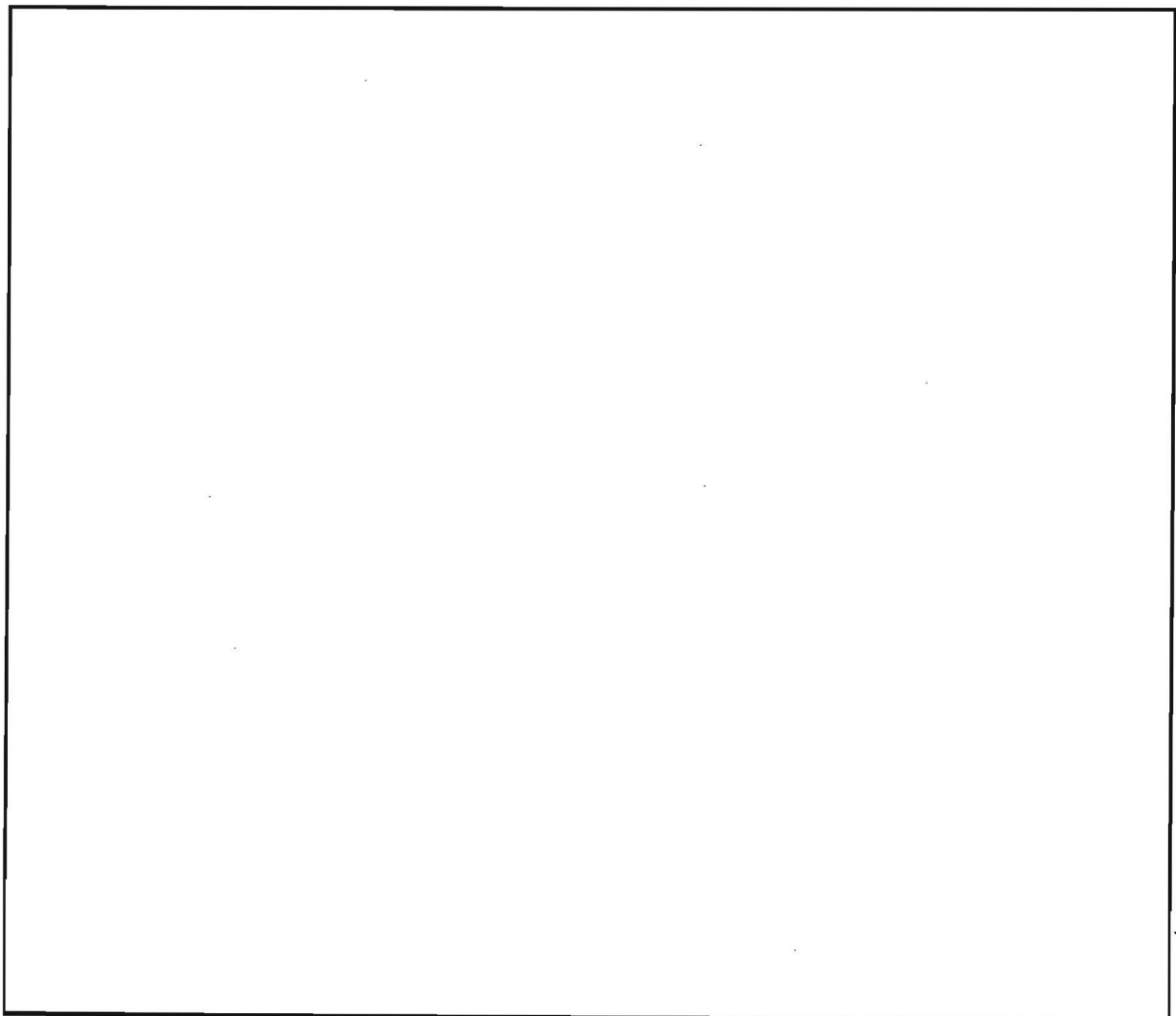
EGuardian-828

enforcement analysis, and all will receive online security and privacy training. Careful auditing is performed throughout the work-flow process.

System Status: The eGuardian system development continues to progress on schedule. Initial beta testing began in July 2008 at the Richmond Fusion Center. On 07/10/2008, the FBI's Security Division received "Authority to Operate". The eGuardian Privacy Impact Assessment (PIA) was approved by DOJ on 11/25/2008. There has been a phased deployment of eGuardian starting with initial pilot locations in California, Virginia and Florida. Additional deployments have been made to numerous federal, state and local agencies as well as FBI field offices.

In support of the 2009 Presidential Inauguration, eGuardian has been deployed to the Washington Field Office and the Washington Regional Threat and Analysis Center for utilization as the main reporting system for all unclassified threats with a potential terrorism nexus.

Nationwide implementation continues along with additional system enhancements in future releases throughout Fiscal Year 2009, to include Interface for First Responders and Private Security, Geo-Spatial Mapping Tools, Advanced Search, and Analyst Reporting.

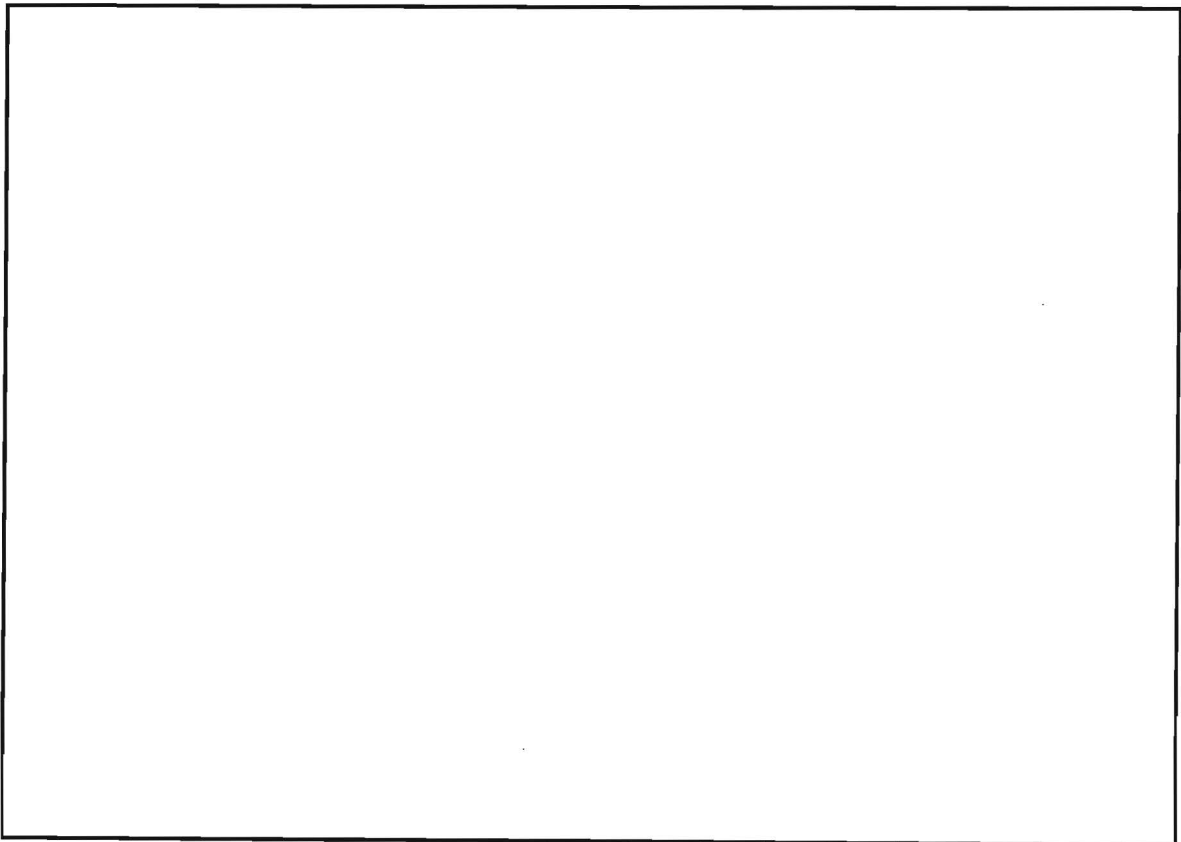


b7E

The eGuardian system will be an unclassified, law enforcement sensitive version of Guardian. eGuardian will be accessible via Law Enforcement Online (LEO), and when fully implemented, will have many of the Guardian features that allow state, local and tribal law enforcement partners to share threat data electronically. eGuardian empowers agencies that do not have daily access to Guardian through FBI-partnered Fusion Centers and Joint Terrorism Task Force (JTTFs), to collect, share and analyze threat data in an efficient and expedient manner.

eGuardian will enable users to enter, view, search, and create useful reports from threat data input by law enforcement officers and from FBI unclassified threat incidents "pushed out" from Guardian. Unclassified information from the Guardian system will be routinely added to the eGuardian application to enhance information sharing. This is a new and innovative approach to information sharing that is desperately needed.

eGuardian 1.0 is an initial, basic capability to enable information sharing with all federal, state, local, and tribal law enforcement. The current process is for state and local law enforcement to report their suspicious activities up through their local Fusion Center if one exists. Otherwise, TMU will function as the virtual Fusion Center for those agencies who are not aligned with a specific Fusion Center. Future versions of eGuardian will likely contain additional workflow that allows supervisory chains and the Fusion Centers to play more specific roles in the processing of suspicious activity reports.



b7E