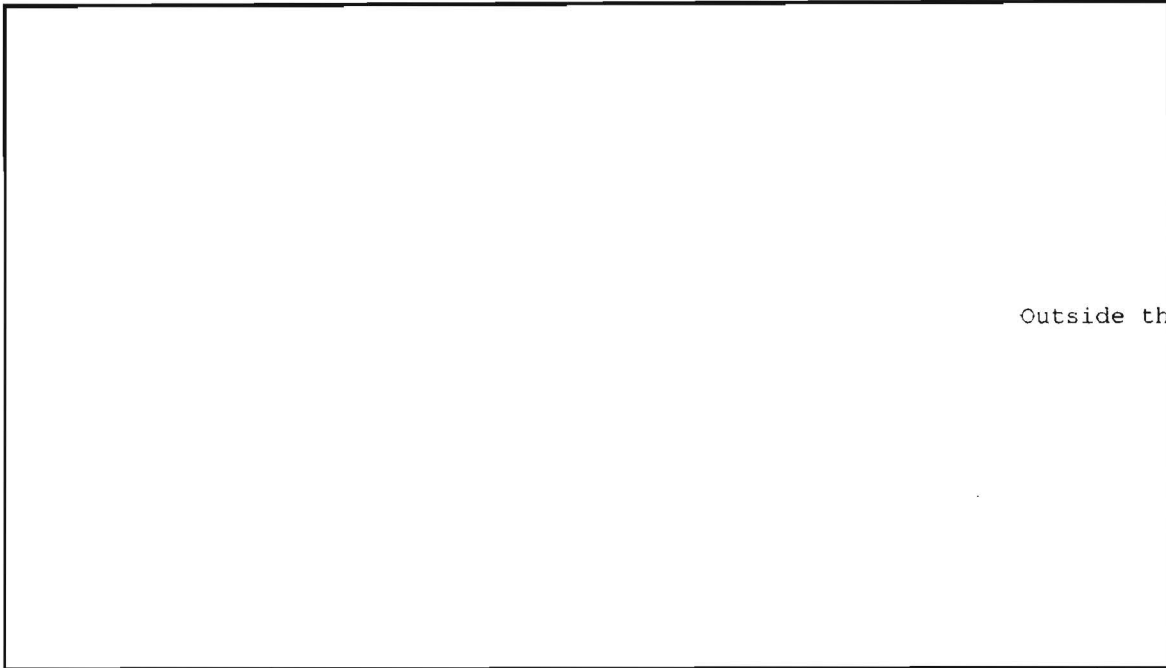


THE GUARDIAN/eGUARDIAN PROGRAM



Outside the Scope

eGuardian is a Secure But Unclassified (SBU), user-friendly system, implemented to share potential terrorist threats, terrorist events, and suspicious activity information among state, local, tribal, and federal law enforcement partners, along with state fusion centers, regional intelligence centers, and the FBI Joint Terrorism Task Forces (JTTFs). eGuardian is an enhancement to the secret level Guardian system, and works in tandem with Guardian to provide unsurpassed access to Suspicious Activity Reports (SARs) and intelligence analysis for the law enforcement community. eGuardian is intended to function as an alert, recording and reporting system for all law enforcement (LE). eGuardian allows recognized LE entities to record suspicious activity or threat information with a potential nexus to terrorism, in a standardized format using a pre-defined business process flow, and submit the information for review and analysis at the local agency, regional or state fusion center, and FBI JTTF.

eGuardian provides a near real-time information sharing environment and is available at no cost to law enforcement partners via Law Enforcement Online (LEO). In addition to the potential terrorist threats, terrorist event, and suspicious activity information, eGuardian provides the ability to attach documents, photo images, videos, and audio clips. Nationwide implementation of eGuardian continues, along with additional system enhancements in future releases throughout Fiscal Year 2010. As of



b7E

EGuardian-717

When incidents are created in eGuardian, the "owner" of the incident is the originating and/or submitting agency. The incident must be approved by a supervisor within the submitting agency and by an eGuardian Administrator in the appropriate fusion center, before it is shared with other eGuardian users and the FBI JTTF via electronic passage to Guardian. Not all eGuardian incidents will require investigative action. Many incidents are not actionable, however, may be important for situational awareness and analytical value.

Information ingested into Guardian from eGuardian assists in the assessment of terrorism-related threats and suspicious activities, enabling analysis of links, relationships, and matches among numerous data elements. The eGuardian Program Team designed and incorporated tools in eGuardian that enable analysts and investigators to quickly develop leads, identify potential suspects, and to share vetted information with other law enforcement agencies 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.

The Guardian/eGuardian Program is an integral component of the Nationwide Suspicious Activity Reporting Initiative (NSI). The NSI is a comprehensive effort, involving Federal, State, local and tribal authorities, to build upon existing capabilities and establish a unified, nationwide process for sharing terrorism-related SARs. The NSI is an outgrowth of a number of separate but related activities that respond directly to the mandate to establish a "unified process for reporting, tracking, and accessing [SARs]" as called for in the National Strategy for Information Sharing (October 2007).

The NSI has been managed by the Program Manager for the Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence (ODNI). It is anticipated that by March 1, 2010, responsibility for the NSI will be transitioned to the NSI Program Management Office (NSI-PMO) within the U.S. Department of Justice. The NSI-PMO will be staffed by personnel representing the FBI, DHS, PM-ISE, and state and local law enforcement.

Authority for information sharing initiatives is contained in the intelligence Reform and Prevention Act of 2004 (IRPTA), Section 1016. The need for an NSI PMO was formally identified in an October 28, 2008, memorandum from the PM-ISE to the Deputy Director for Management at the Office of Management and Budget (OMB), entitled "2008 Information Sharing Environment (ISE) Program Review Finding and Recommendation." ISE Programmatic Guidance for FY2011 issued by the White House on July 28, 2009, also specifically calls on DOJ and DHS to "support the development of recommendations for Deputies regarding the establishment and functions of an interagency SAR Program Management Office that will oversee the Nationwide SAR Initiative." Continued support and integration of eGuardian into the NSI is critical to ensure that all SAR information in eGuardian will be accessible through the Information Sharing Environment (ISE) Shared Spaces and vice versa.

EGuardian-718

The eGuardian Program Team worked closely with the Department of Defense (DoD) in supporting their evaluation of the eGuardian system as an appropriate replacement of the DoD's defunct TALON threat management system. The team spent countless hours working with key DoD contacts and incorporated eGuardian Program Team members, who served as liaisons between DoD and eGuardian system developers. The team managed to incorporate numerous DoD requirements into the system. The voluminous amount of personnel resources invested with DoD resulted in their selection of eGuardian as the interim replacement for TALON. The team's work culminated in a Pentagon briefing of the U.S. Army General in charge of the Army's Military Police and Criminal Investigative Division. DoD utilizes eGuardian to track and manage force protection threats worldwide.

From fiscal year 2005 to present, the FBI has only invested approximately \$15 million of its Counterterrorism budget, to design, build, deploy, and maintain both the Guardian and eGuardian systems. It is our belief that the FBI has utilized the aforementioned funds to provide a valuable service, which supports the primary mission of the FBI, and enables critical information sharing with local, state, tribal and federal law enforcement throughout the United States and internationally.

EGuardian-719