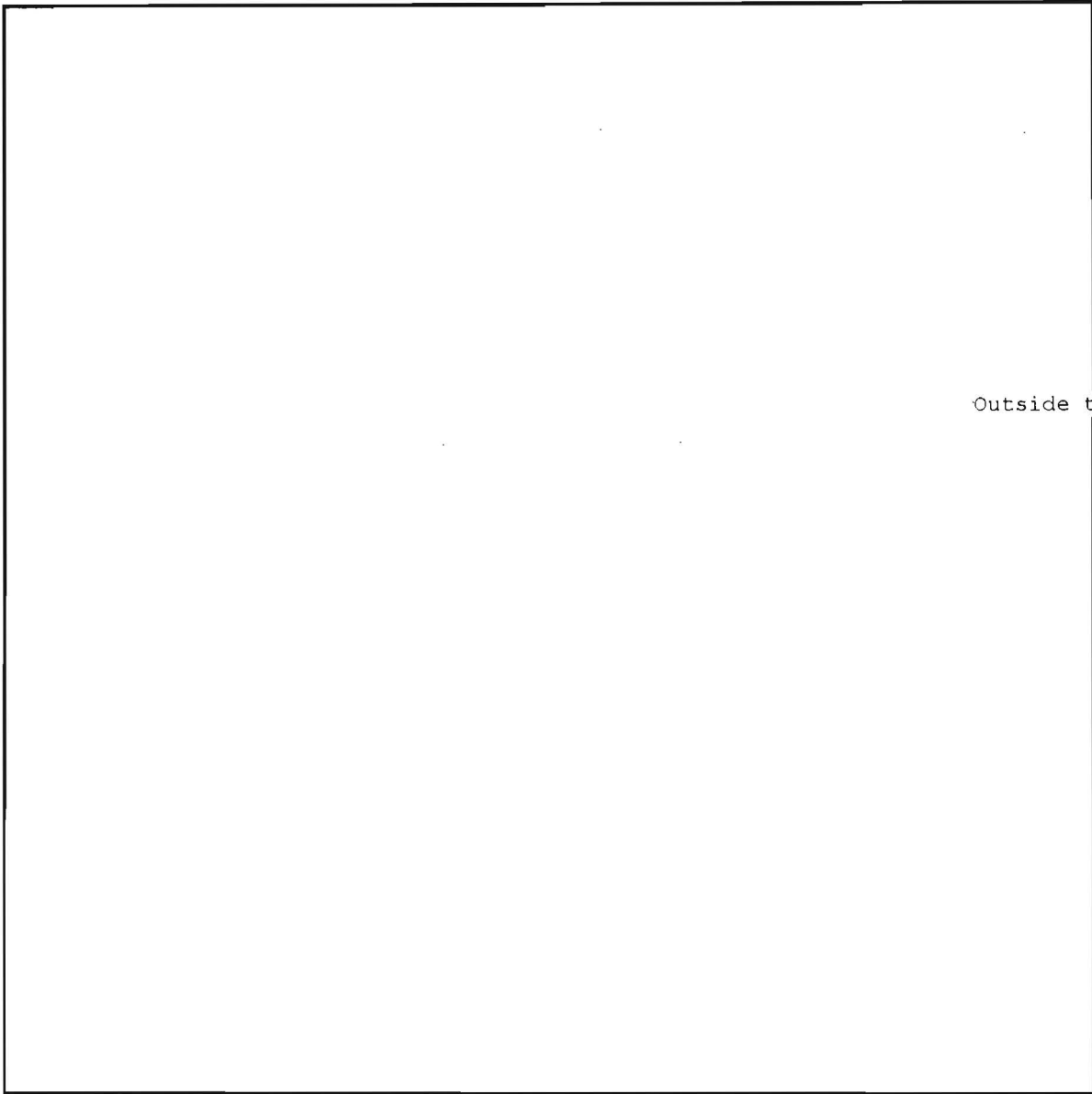


FOR OFFICIAL USE ONLY



Federal Bureau of Investigation
DoD Guardian/ eGuardian Use

Guardian



Outside the Scope

EGuardian-722

Control #:6/13/08

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY



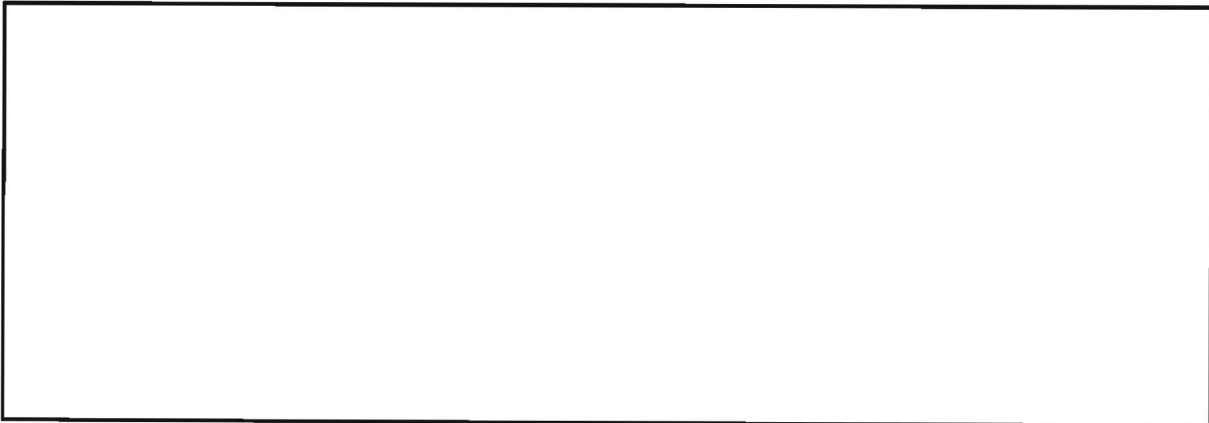
Outside the Scope

eGuardian

(U) eGuardian is an SBU, user-friendly enhancement to the Guardian Program. eGuardian was implemented to share potential terrorist threats, terrorist event, and suspicious activity information among state, local, tribal, and federal law enforcement partners, in conjunction with state fusion centers, regional intelligence centers, and the FBI Joint Terrorism Task Forces (JTTFs). eGuardian bridges the gap between the secret level Guardian system on FBINet and the SBU law enforcement environment, via Law Enforcement Online (LEO). eGuardian is securely linked to Guardian, and provides a technical solution for information to be electronically shared among eGuardian users and the JTTFs. 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 JTTF.

(U) eGuardian is the only system that shares potential terrorist threats, events, and suspicious activity information among local, state, tribal, and federal law enforcement partners, along with state fusion centers, Urban Area Intelligence Centers, and the JTTFs. eGuardian is also the only system that allows law enforcement partners to access unclassified data from the Guardian Threat Tracking System.

(U) eGuardian provides a near real-time information sharing environment and is available at no cost to law enforcement partners via LEO. The eGuardian Special Interest Group (SIG) is moderated by FBI personnel assigned to the Threat Monitoring Unit (TMU). In addition to the potential terrorist threats, events, and suspicious activity information, eGuardian provides the ability to attach documents, images, videos, and audio clips to an incident.



b7E

EGuardian-723

Control #: 6/13/08

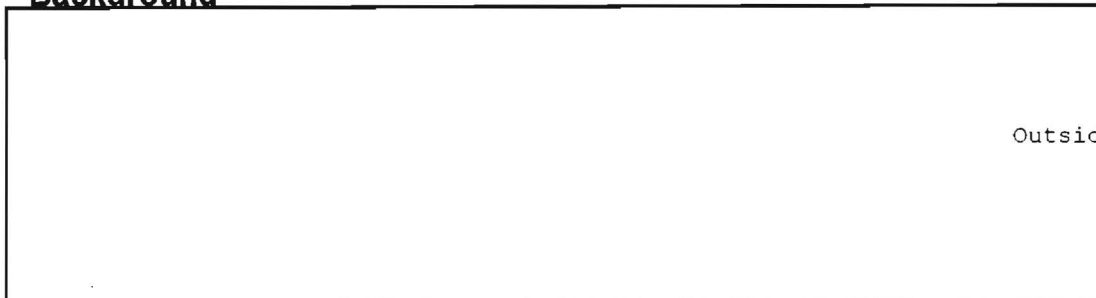
FOR OFFICIAL USE ONLY

e-Guardian Functional Description

Purpose

To provide a functional description of a new, unclassified terrorism-related incident tracking system, called e-Guardian. e-Guardian facilitates the sharing of information between other federal, state, local, and tribal law enforcement agencies with the FBI regarding suspicious activities and threats.

Background



Outside the Scope

The e-Guardian application, the unclassified version of Guardian, will be hosted on Law Enforcement Online (LEO) and will have many of the Guardian features that allow other law enforcement partners to share threat data electronically with each other and the FBI. e-Guardian empowers agencies that do not have 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. This is a new and innovative approach to information sharing that is desperately needed.

e-Guardian 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 e-Guardian application to enhance information sharing. Local law enforcement partners will have the ability to decide whether their entered incident should remain locally in e-Guardian or be shared with the FBI for potential upload to the Guardian system.

This is an incident reporting system of suspicious terrorism-related activity. Urgent law enforcement matters, investigative issues, and classified matters should continue to be handled or investigated through existing, established FBI and law enforcement channels. e-Guardian is intended to supplement and enhance, not replace, existing Fusion Center and JTTF coordination, while allowing small police departments a forum to participate in the global war on terrorism and larger departments a repository for incident information that when judged in a vacuum, might not trigger contact with a local JTTF.

e-Guardian data is transformable and transportable, allowing it to be moved into formats that can be easily combined with other software applications used by local and state law enforcement partners. In other words, for the law enforcement agencies who already have their own incident tracking system; e-Guardian data can be easily extracted and loaded into a local application. Law

EGuardian-731

e-Guardian Functional Description

enforcement agencies that do not have an incident tracking system can utilize e-Guardian to manage their information. The data is best described as strategic data that may require linkages to other law enforcement data before it becomes actionable information. The flexibility e-Guardian provides in handling the data allows integration and analysis with other data sources to search for trends, patterns, and connections. Users are able to manipulate the data into new data sets to enhance analysis and to meet evolving threat patterns. The data can be viewed, analyzed and used in many ways.

Since September 2005, the FBI has been posting unclassified suspicious activity and threat information reports to the e-Guardian Special Interest Group (SIG) website on LEO. These Threat Incidents Reports (TIRs) are posted in an effort to provide unclassified intelligence to law enforcement partners and to get SIG members familiar with interacting with the e-Guardian web-site in anticipation of the system's release. When the e-Guardian system is ready for deployment, it will be accessed from this location. The currently-posted TIRs are produced weekly by the FBI's Threat Monitoring Unit (TMU), National Threat Center Section, Counterterrorism Division. This is a Law Enforcement Sensitive general report, intended to be shared with the entire law enforcement community. The TIRs summarize significant unclassified threat entries reported through the Guardian system, and organize the threats by infrastructure sector. Local law enforcement partners can obtain admission to the e-Guardian SIG through LEO by making an access request to TMU, the Guardian/e-Guardian program management office for the FBI. LEO access can be obtained from the LEO administrator, the CJIS Division.

e-Guardian will be deployed on LEO before the end of 2007. When the system is available, users will be able to access the system to enter incidents, view FBI incidents, search the data, or build their own customized reports. The user will be able to transfer e-Guardian data into other software applications such as Microsoft Office and i2 using its data export capabilities. All that is required is a computer with Internet access, including from a laptop operating in a wireless environment, a LEO account, membership in the e-Guardian SIG, and agreement with the guidelines for sharing the data. E-Guardian screens contain numerous prompts and drop down menus to assist the user in introducing data into the system in a uniform manner which will greatly enhance subsequent searches.

An aggressive training and marketing strategy is planned to properly emphasize the application features and will dovetail with a computer based training module on LEO. E-Guardian will dramatically increase the information sharing capability of terrorism-related incidents across the entire law enforcement community.

For more information about e-Guardian, contact SSA Jeffrey Danik, e-Guardian PM, 571-280-6477.

EGuardian-732

e-Guardian

e-Guardian will facilitate the sharing of information between Joint Terrorism Task Forces (JTTF) and other federal, state, local, and tribal law enforcement agencies regarding suspicious terrorism related activities and threats. E-Guardian makes threat information immediately available to authorized users, allows all users to search all incidents for trends and patterns, and assists in ensuring that no suspected terrorism incident is left uninvestigated. The e-Guardian application will be hosted on Law Enforcement Online (LEO) and will allow law enforcement partners to share threat data electronically with each other. e-Guardian empowers agencies that do not have access to JTTF-partnered Fusion Centers or Joint Regional Intelligence Centers (JRICs) to collect, share and analyze threat data in an efficient and expedient manner. This is a new and innovative approach to information sharing that is desperately needed. e-Guardian 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 the internal JTTF/FBI threat tracking system called Guardian. Unclassified information from the Guardian system will be routinely added to the e-Guardian application to enhance information sharing. Law enforcement partners will have the ability to decide whether their entered incident should remain under their control for resolution in e-Guardian or be referred to the JTTF/FBI for resolution.

e-Guardian is intended to supplement and enhance, **not replace**, existing Fusion Center/JRIC and JTTF coordination. E-Guardian provides smaller police departments, who are in States that do not have a formal Fusion process, a forum to participate in the global war on terrorism and offers them and Fusion Centers a repository for incident information that when judged in a vacuum, might not trigger contact with a local JTTF.

e-Guardian will be deployed on LEO. When the system is available, users will be able to access the system to enter incidents, view certain Unclassified FBI incidents, search the data, or build their own customized reports. The user will be able to transfer e-Guardian data into other software applications such as Microsoft Office and i2 using e-Guardian data export capabilities. E-Guardian screens contain numerous prompts and drop down menus to assist the user in introducing data into the system in a uniform manner which will greatly enhance subsequent searches.

For more information about e-Guardian, contact FBI SSA [REDACTED]
e-Guardian Project Manger, [REDACTED]

b6
b7C

EGuardian-733