#3

eGuardian

December 10, 2008

Summary

Due to the mandate expressed in the Intelligence Reform and Terrorism Prevention Act, in other statutes and Executive Orders, and in the National Strategy for Combating Terrorism to share terrorism information with federal, state, local, and tribal law enforcement partners, the FBI, CTD has created an unclassified version of its Guardian program--called eGuardian--that will provide participating partners with a suspicious activity reporting (SAR) system accessible via Law Enforcement Online. The eGuardian system will facilitate situational awareness with respect to potential terrorism threats and activity. Sharing information within the eGuardian network should eliminate the jurisdictional and bureaucratic impediments that otherwise delay communication and dissemination of information that could potentially affect the nation's security posture.

The eGuardian system was envisioned as a tool for state and local police departments to share information with a potential nexus to terrorism amongst their own agencies, with Fusion Centers, other federal agencies, and the FBI. As eGuardian development has progressed, the need for such a system to exist has become apparent. This is evidenced by the efforts of multiple jurisdictions at the state, local, and federal levels to create their own suspicious activity and threat tracking systems. By utilizing the eGuardian system, the United States law enforcement community will enjoy a previously unrealized degree of connectivity with regard to the collection and dissemination of suspicious activity and threat reporting, regular push down of unclassified SAR from the FBI, and an electronic internet based link to the Joint Terrorism Task Forces (JTTFs). The eGuardian system will essentially provide state and local users a uniform platform to cause actionable information with a potential terrorism nexus to be analyzed at the state Fusion Center level and reported to the JTTFs via the classified Guardian system.

System Overview

The eGuardian system is a sensitive but unclassified (SBU) version of the FBI's Guardian Threat Tracking System. Unlike Guardian, incidents will not be investigated or "worked" in eGuardian. The eGuardian system will electronically record SAR and terrorist threat information with a potential nexus to terrorism gathered by law enforcement agencies. The system is designed to act as a standardized SAR system that will allow multiple agencies to consolidate existing disparate reporting systems that, in many cases, have no connectivity with other agency SAR systems. Furthermore, eGuardian will be populated with SBU data flowing into the Guardian system completing the cycle of report sharing between the FBI and our state, local, tribal and federal partners.

The eGuardian system helps fulfill the mandates expressed in the Intelligence Reform and Terrorism Prevention Act of 2004, in other statutes and Executive Orders, and in the National Strategy for Combating Terrorism. A key directive to the FBI was to develop a system to share terrorism information with our federal, state, local, and tribal law enforcement partners. The eGuardian system is the only SAR system that communicates directly with the FBI's JTTFs and is therefore, the premier SAR tool.

"Suspicious activity" is defined as *observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention.* This definition of suspicious activity is taken directly from the Program Manager/Information Sharing Environment (PMISE) for consistency across the affected law enforcement communities. Suspicious activity may include surveillance, cyber attacks, probing of security and photography of key infrastructure facilities.

SARs that are entered into the eGuardian system from federal entities will be analyzed initially by the FBI's National Threat Center Section, Threat Monitoring Unit (TMU) to determine whether sufficient facts exist to warrant the information being placed into the Guardian system for investigation. TMU will, in effect, act as an eFusion Center for federal agencies utilizing the eGuardian system and for law enforcement agencies that do not report to an established state administered Fusion Center. SARs from federal, state, local, and tribal law enforcement that are reported to eGuardian will pass through a state Fusion Center or similar analytical construct prior to being passed to the Guardian system for assignment to a JTTF or an FBI Guardian squad. In all cases of data ingest, trained analyst or law enforcement personnel will make the judgement that the information rises sufficiently to the level that a report should be added to the eGuardian and Guardian systems.

Personally identifiable information (PII) to be collected will include all available identifiers regarding the subject of a report or incident. Incidents created within eGuardian will be initially retained in the system as a "DRAFT" report. The eGuardian DRAFT reports will only be viewable by the creator of the incident, and the creator's supervisor, if applicable. If an agency chooses to share a report, they will refer the report to a Fusion Center. At that point, the report will be visible to the submitting agency and the receiving Fusion Center only. This workflow limits the unvetted exposure of PII to the eGuardian user community. If the Fusion Center/eFusion Center determines the report has a potential nexus to terrorism, that entity will refer the report to Guardian. Within the eGuardian system, the report status changes to "REFERRED" and the incident is electronically uploaded to Guardian from eGuardian for assignment to a JTTF. While in referred status, the incident becomes viewable to all eGuardian users. Simultaneously, "referred" incidents will be viewable to users of Guardian and clearly marked to indicate the report's eGuardian origin . Incidents that are determined to have no nexus to terrorism will be CLOSED and subsequently DELETED from the eGuardian system to ensure that personal data is not being needlessly stored.

Coordination with PMISE, National SAR Initiative, and Shared Spaces Evaluation Environment

CTD has coordinated closely with the PMISE which has been working on the National Suspicious Activity Reporting Initiative (NSI). The goal of the NSI is that Federal, State, local, tribal and law enforcement organizations across the country participate in a standardized, integrated approach to documenting, processing, analyzing, and sharing terrorism-related suspicious activity. The NSI is an umbrella initiative encompassing multiple complementary efforts by federal, state, local and tribal agencies to detect and prevent terrorist activities and to bring perpetrators to justice. The emphasis is on improving and standardizing policies, processes, and procedures for sharing SARs with a potential terrorism nexus rather that employing specific automated tools or techniques.

The NSI Evaluation Environment (EE) provides an opportunity to test systems for implementing these goals. Two systems, in particular, will be evaluated in 2009: ISE Shared Spaces and the FBI's eGuardian.

- The ISE Shared Spaces were developed in an initiative to provide "a decentralized, distributed, and coordinated environment," for sharing of terrorism related information as directed by Congressional language. This system relies upon individual agency's own system/processes to post or access SARs through dedicated servers located at fusion centers. Accessible by other ISE participants, the information in an ISE Shared Space remains under the management and control of the organization that originally submitted the information to the ISE, i.e, the fusion center or agency that determined that the activity met the criteria for designation as an ISE-SAR.

- The eGuardian system is part of the a national FBI Guardian program designed to record and share threat-related, suspicious activity information about possible terrorist activities of groups or individuals among LE in all relevant jurisdictions. Guardian is the FBI's classified threat management and suspicious activity system. It is available to all FBI Field Offices and Legat locations, Joint Terrorism Task Forces (JTTFs), Fusion Centers (with FBINet access), and other government agency (OGA) partners located in shared facilities. The eGuardian system was created to facilitate sharing of suspicious activity reporting and threat information in the unclassified realm and to extend this communication network to organizations not connected to fusion centers, shared facilities, or classified systems. The eGuardian system is accessed via a portal on the Law Enforcement Online (LEO) network housed on the internet. It allows users to apply business processes customized for each agency or organization to share information (SARs, threat, and analysis or to discover information through federated searches.

Both systems enable improved sharing of terrorism-related SARs; both implement the NIEM SAR IEPD; both systems incorporate provisions that help protect privacy and civil liberties, and both systems

make standardized terrorism-related information accessible to authorized ISE users in the other system. In each system, threat-related information and analysis can be provided directly to Joint Terrorism Task Forces and broadly shared via federated queries.

eGuardian Status

The eGuardian system development continues to progress on schedule. Our initial beta testing began in July 2008. eGuardian has obtained authority to operate from the FBI's Security Division, effective July 10, 2008. The tentative deployment strategy of eGuardian is as follows:

October 2008: Initial deployment of eGuardian 1.0: National Capitol Regional Intelligence Center, Alexandria, VA; Virginia Fusion Center, Richmond, VA; the Washington Regional Threat and Analysis Center, Washington, DC; the Federal Air Marshals Service; the Washington, D.C. Capitol Police Department; Los Angeles Joint Regional Intelligence Center (JRIC) and Sacramento Regional Terrorism Threat Assessment Center (RTTAC); the Department of Defense (DoD) and the FBI Public Access Center Unit.

Fall and Winter 2008: Portland (Oregon), Seattle (Washington), Tallahassee (Florida), Newark (New Jersey), Boston (Massachusetts), Phoenix (Arizona), Denver (Colorado) Organizational Pilot set-up.

January 2009: eGuardian 1.1 based on evaluation period assessment and user feed-back.

March 2009: eGuardian 1.2 based on evaluation period assessment and user feed-back.