U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

April 16, 2010

MS. LAURA ROTOLO
ACLU OF MASSACHUSETTS
211 CONGRESS STREET
BOSTON, MA 02110

FOIPA Request No.: 1141760- 000
Subject: JTTF/ DOCUMENTS DISCUSSING RULES AND GUIDELINES FOR JTTF COMPLIANCE WITH 28 CFR PART 23

Dear Ms. Rotolo:

The enclosed document was reviewed under the Freedom of Information/Privacy Acts (FOIPA), Title 5, United States Code, Section 552/552a, and is being released to you in its entirety. This is in response to your FOIPA request noted above.

You have the right to appeal any denials in this release. Appeals should be directed in writing to the Director, Office of Information Policy (OIP), U.S. Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, D.C. 20530-0001. Your appeal must be received by OIP within sixty (60) days from the date of this letter in order to be considered timely. The envelope and the letter should be clearly marked "Freedom of Information Appeal." Please cite the FOIPA Request Number assigned to your request so that it may be identified easily.

Very truly yours,

David M. Hardy
Section Chief
Record/Information
Dissemination Section
Records Management Division

Privacy Impact Assessment for the eGuardian Threat Tracking System

Responsible Officials
Counterterrorism Division
Program Manager
Gerald J. Rogero, III
Threat Monitoring Unit (TMU)
571-280-6372

System Developer
Christopher Light
Foreign Terrorist Tracking Task Force (FTTTF)
703-682-4662

Reviewing Officials
David C. Larson
Chief Privacy and Civil Liberties Officer
Federal Bureau of Investigation

Vance E. Hitch
Chief Information Officer
Department of Justice

Approving Official
Kenneth P. Mortensen
Acting Chief Privacy Officer and Civil Liberties Officer
Department of Justice

November 25, 2008

INTRODUCTION

Overview

The National Threat Center Section (NTCS) in the FBI's Counterterrorism Division is the focal point for all threat information, preliminary analysis, and assignment for immediate action of all emerging International Terrorism and Domestic Terrorism threats incoming to the FBI. Within NTCS, the Threat Monitoring Unit (TMU) has the primary responsibility for supporting the FBI's role in defending the United States against terrorism threats. Through coordination with FBI Field Offices, Legal Attaches, and other government agencies, TMU collects, assesses, disseminates, and memorializes all threat information collected or received by the FBI. A companion unit to TMU, the Threat Review Unit (TRU), analyzes the threat information that is collected in order to identify trends and prepares informational products that can be shared.

To help it accomplish its work, in 2003, TMU developed the Guardian Program.[1] Guardian is an information technology system maintained at the Secret level that allows TMU to collect suspicious activity reports (SARs) made to the FBI and review the SARs in an organized way to determine which ones warrant additional investigative follow-up. Guardian's primary purpose is not to manage cases, but to facilitate the reporting, tracking, and management of threats to determine within a short time span (30 days or less) whether a particular matter should be closed or referred for an investigation. Guardian also facilitates the TRU's work in performing its analytical functions because the reports are available for pattern and trend analysis.

Because of the mandate, expressed in the Intelligence Reform and Terrorism Prevention Act as well as in other statutes and Executive Orders and in the National Strategy for Combating Terrorism, to share terrorism information with other federal, and state, local and tribal (SLT) law enforcement partners, the FBI now proposes to create an unclassified version of its Guardian Program – called eGuardian – that will provide participating partners with access to a reporting system to be hosted on a secure but unclassified Internet network that will be accessed through Law Enforcement Online (LEO). The SARs that are contributed to eGuardian, after initial approval, will be accessible to specially-vetted representatives of other federal law enforcement partners and SLT law enforcement partners. These SARs should help facilitate situational awareness with respect to potential terrorism threats. Sharing these reports should eliminate the jurisdictional and bureaucratic impediments that otherwise delay communication of this important information that is necessary to enhance our national security posture.

Information Sources

The threat information to be contributed to eGuardian may come from three sources: (1) unclassified information from the FBI's Guardian system; (2) reports from other federal agencies with law enforcement functions, including components of the

[1] The Guardian Program was the subject of a Privacy Impact Assessment dated April 13, 2005.

Department of Homeland Security[2] and law enforcement investigative services within the Department of Defense;[3] and (3) SARs contributed by SLT law enforcement.

Unclassified information from the Guardian system that appears to have a potential nexus to terrorism will be passed down to eGuardian, where it will be available for viewing by the participants of eGuardian, including those members of SLT law enforcement and representatives of other federal law enforcement agencies that have been given permission to access the eGuardian system.

For the information coming from other federal agencies with law enforcement functions, including FBI unclassified reporting passed through Guardian Express, TMU will conduct the initial screening of federal suspicious activity reports, other than reports by law enforcement investigative services within DoD. Suspicious activity reports from law enforcement investigative services within DoD will be analyzed in a DoD fusion center-like organization for a further determination whether the information warrants contribution to eGuardian (labeled as the Shared Data Repository (SDR) on Diagram 1.a) and then on into Guardian.

Suspicious Activity Reports from SLT partners will be submitted to the appropriate State or Local Fusion Center for a similar analysis there. If the Fusion Center accepts a report as demonstrating a potential nexus to terrorism, it will be submitted to the SDR and then on into Guardian for the FBI to analyze further to determine if investigative action at the Federal level is warranted. Additionally, once the report is in the SDR, it will be available for viewing by the participants of eGuardian.

From each of these sources, those reports that appear to have a potential nexus to terrorism will be added to the Guardian system for further analysis. Incidents and threats that are found to warrant investigation will be assigned, via Guardian, to a member of one of the FBI's Joint Terrorism Task Forces (JTTFs). Nationwide, all 56 FBI field divisions maintain at least one JTTF. The JTTFs are comprised of SLT law enforcement officers who are deputized as federal agents, as well as law enforcement agents from other federal agencies, including the Department of Homeland Security and the Department of Defense. The JTTFs have the primary responsibility for investigating terrorist threats, events, and suspicious activities with a potential nexus to terrorism.

The eGuardian system will be used to record, review, sort, and prioritize these counterterrorism threats and suspicious activity incidents and present the information to law enforcement partners who will access the eGuardian SDR through a Special Interest Group accessed through LEO. Law enforcement agencies that have contributed information will have read and write access to their reports in the SDR in order to update them as necessary. Other law enforcement partners will have read-only access to the

---

[2] These include the Federal Air Marshals Service, Immigration and Customs Enforcement, Customs and Border Protection, and the United States Coast Guard.

[3] These include the Army Criminal Investigation Command (CID), the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations. Other DOD components with force protection law enforcement arrest authority may also participate in eGuardian, such as the Pentagon Force Protection Agency.

SDR to ensure appropriate dissemination of these counterterrorism threats and suspicious activity incidents.

Review Process

Throughout the initial threat reporting process, regardless of where the report originates, if a determination is made of "no nexus to terrorism," the information will not be added to the eGuardian SDR. Additionally, at the Fusion Center level, the information will be deleted. If a clear determination is made of "a nexus to terrorism," the information will be passed along to the eGuardian SDR for further dissemination and then on to Guardian for analysis. If no determination can be made regarding "a nexus to terrorism," but neither can the nexus be discounted, the information will be added to the eGuardian SDR for pattern and trend analysis.

In keeping with the retention period currently in effect for state criminal intelligence systems under 28 C.F.R. Part 23, suspicious activity reports in this third category (reports for which a determination cannot be made whether or not a nexus to terrorism exists) will be retained for a period of five years and will be used for analytical purposes and/or to demonstrate trends. eGuardian considers all reports submitted to the system to be the property of the submitting agency; therefore, should a submitting agency desire that a report be removed from the system prior to the five-year mark, the report will be removed. Otherwise these reports also can be available for trend and other analyses.

User Access/Security

The eGuardian system will ensure consistency of process and of handling protocols by using a uniform user agreement for each agency or law enforcement entity that connects to eGuardian through LEO. By signing the user agreement, the parties will agree to the Fusion Center or TMU policies, which reflect the conditions of use and privacy and security requirements of eGuardian. All users will be required to assent to these rules of behavior each time they log on to the system. Additionally, all users will be required to complete robust system training that will incorporate eGuardian policies and procedures concerning privacy and civil liberties. Audit controls will be employed to ensure that the use of eGuardian is consistent with its intended purpose.

The following diagram (Diagram 1a) provides an overview of the eGuardian system described in this Privacy Impact Assessment. Data is input at an initial level but reviewed at a Fusion Center or similar entity before being passed to eGuardian if the information appears to be linked to terrorism. The "Agency Data Input Zone" represents law enforcement contributors of suspicious activity reports with a potential nexus to terrorism. The Fusion Center Management Zone represents the vetting that must occur before these reports are shared with eGuardian participants. The eGuardian Exchange Zone is where this information sharing will actually occur, once a determination has been made that the report has a potential nexus to terrorism. The FBI's role is to serve as both a contributor of information from its Guardian system and a recipient of eGuardian reports that warrant additional investigation at the Federal level.

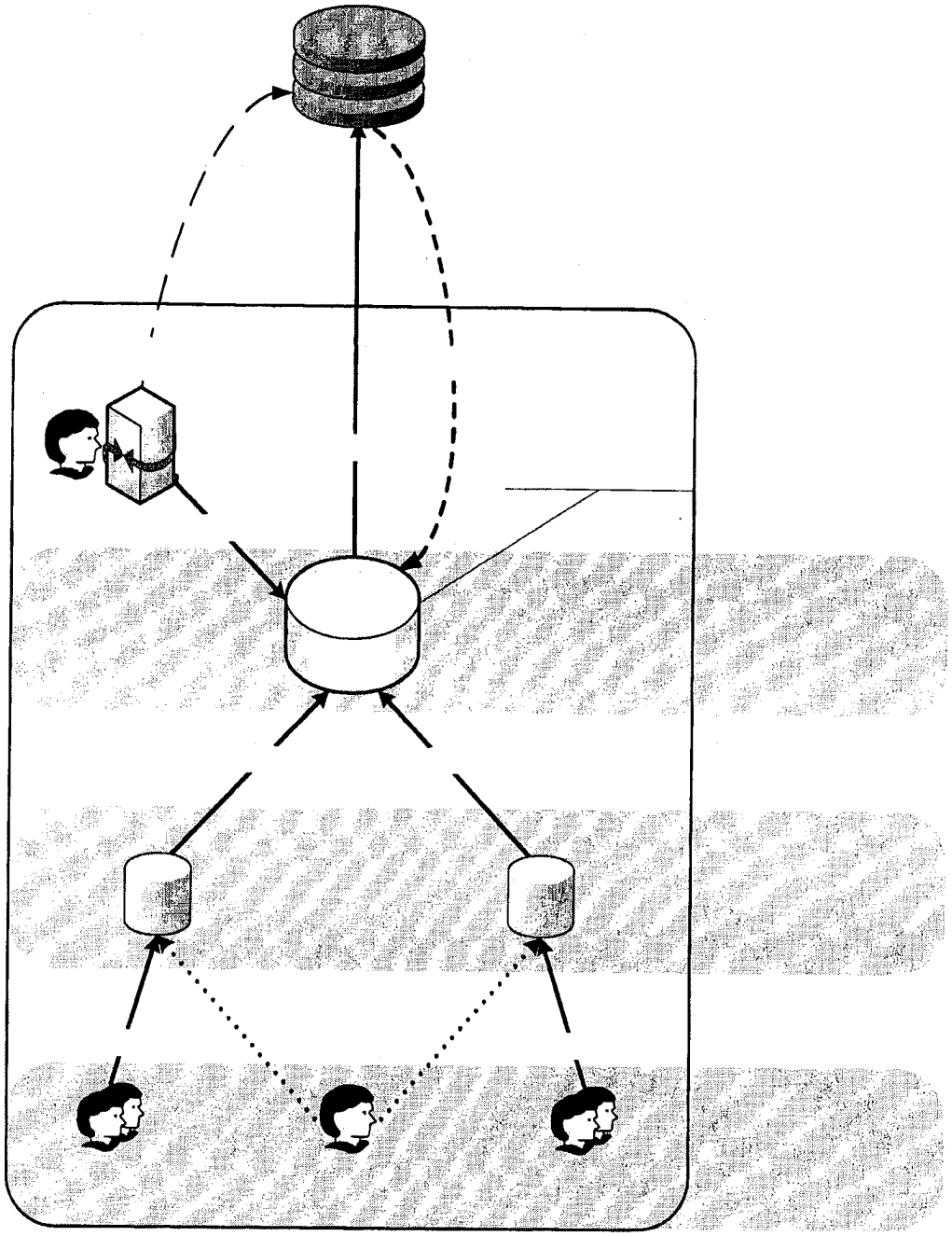

Diagram .1a

Direct Report

Section 1.0
The System and the Information Collected and Stored within the System

1.1 What information is to be collected?

eGuardian will collect terrorism threat information and/or suspicious activity information having a potential nexus to terrorism. "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 is consistent with the definition utilized by the Program Manager/Information Sharing Environment (PM/ISE). Suspicious activities may include surveillance, cyber attacks, probing of security and photography of key infrastructure facilities. Personally identifiable information (PII) to be collected will include all available identifiers regarding the subject of a report or incident, such as name, date and place of birth, unique identifying numbers, physical description, and similar attributes.

1.2 From whom is the information collected?

Suspicious activity reports and threats that have a potential nexus to terrorism may be reported to law enforcement from private citizens or may come directly from law enforcement personnel who observe or investigate activities.

1.3 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

FBI suspicious activity reports that are entered into eGuardian at the federal level will have been analyzed initially by TMU to determine whether sufficient facts exist to warrant placement of the information into the system. Suspicious activity reports from SLT law enforcement and other federal agencies will be required to pass through a Fusion Center or similar analytical construct prior to being passed to eGuardian. In all cases of data ingest, trained analysts or law enforcement personnel will make the judgment that the information rises sufficiently to the level that a report should be added to eGuardian.

eGuardian users will be advised in an online tutorial that frequent checking of the database for updates will be necessary, at intervals no less than 30 days, and will be encouraged to ensure that information they have entered initially is supplemented whenever new facts are uncovered. In the work flow that is created for eGuardian, contributors will be able to add notes that help clarify the contributed information.

eGuardian has developed a set of guidelines for the types of information that *cannot* be entered into the system by any participating entity, including the FBI. For example, no entry may be made into eGuardian based solely on the ethnicity, race or religion of an individual or solely on the exercise of rights guaranteed by the First Amendment or the lawful exercise of any other rights secured by the Constitution or the laws of the United States. These restrictions will be prominently displayed when an

individual accesses eGuardian and he or she will have to affirmatively indicate agreement to abide by these rules before being permitted to proceed to view reports.

In addition, the following specific categories of information will not be permitted to be entered into eGuardian: classified information; information that divulges sensitive methods and techniques; FISA-derived information; grand jury information; federal taxpayer information; sealed indictments; sealed court proceedings; confidential human source and witness information; Title III subject and intercept information, and other information that is subject to legal restriction. The eGuardian Program Manager will have personnel assigned to monitor the system to ensure that these categories of information are not included in eGuardian reports.

All information will be subject to threshold screening by the submitting law enforcement officer before being placed in the system and then will be submitted to a Fusion Center, to TMU or to the DOD fusion center-like organization [hereinafter collectively referred to as a "responsible entity"] within the Fusion Center Management Zone (see Diagram 1a) for a decision regarding adding the report to eGuardian. This screening will ensure that trained law enforcement personnel and/or analysts make the initial decision that a report warrants further review. Furthermore, the eGuardian workflow architecture is designed to restrict the ability to view submitted reports to the reporter, the reporter's supervisor, and the approving responsible entity. Incidents submitted to eGuardian will not be viewable to the eGuardian users outside this workflow until the report is approved at the responsible entity level.

Section 2.0
The Purpose of the System and the Information Collected and Stored within the System.

2.1 Why is the information being collected?

The National Strategy for Combating Terrorism recognizes that the war on terror requires greater flexibility and resilience to confront threats facing our nation from a transnational terrorism movement designed to destroy our way of life. The collection of information in eGuardian is consistent with this national strategy and also with the emphasis placed by the President and the Congress on sharing terrorism information with our law enforcement partners. It also recognizes that the police officer on the street is often in the best position to observe suspicious behavior that may have national security implications. eGuardian and Guardian provide a dynamic tool to accomplish this sharing to increase awareness and foster review of threats and suspicious activities in a timely manner so that they can be mitigated appropriately. It is also very important to note that eGuardian is at its very essence, simply a platform to standardize the disparate SAR systems currently utilized by agencies to collect information, which will enhance communication among law enforcement entities as well as situational awareness.

2.2 What specific legal authorities, arrangements, and /or agreements authorize the collection of information?

The FBI's general investigative authority in 28 U.S.C. 533 and its general authority to collect records in 28 U.S.C. 534 provide the statutory basis for the activities ascribed to eGuardian. The FBI is also assigned the lead role in investigating terrorism and in the collection of terrorism threat information within the United States by 28 C.F.R. § 0.85 and Annex II to National Security Presidential Directive 46. In addition, the Intelligence Reform and Terrorism Prevention Act requires the President to establish an information sharing environment for sharing terrorism information in a manner that is consistent with national security and applicable legal standards pertaining to privacy and civil liberties. Further, the President's National Strategy for Information Sharing supports the eGuardian initiative; it identifies suspicious activity reporting as one of the key information exchanges between the Federal Government and State and local partners.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The most significant privacy risk is that information which first appears to be suspicious will turn out, upon further vetting, to be innocuous, resulting in the over collection of data. A related significant risk is that dissemination of personal information will be overly broad and will include agency officials who have no need to know the information, Both risks are mitigated in several ways.

First, a standard definition of what constitutes a suspicious activity will be used by all participating agencies. As mentioned previously, the suspicious activity definition will be the definition currently developed by the PM/ISE. The PM/ISE suspicious activity definition will be augmented by describing the kinds of information that cannot be entered into the system. The definition with these qualifiers will be incorporated into the User Agreement that appears on the LEO eGuardian Special Interest Group page where eGuardian incidents will be placed and individuals accessing the system will have to confirm that they have read and understand the Agreement and agree to be bound by the constraints articulated therein.

Second, eGuardian is intended to function as an alert, recording and reporting system and not as a long-term data repository. As a result, decisions about SARs will be made promptly so that the data can move quickly through the system. All SLT and federal law enforcement agencies with missions that pertain to homeland security will be encouraged to enter terrorism-related threats and suspicious activity incidents into eGuardian for an appraisal by the appropriate Fusion Center, the FBI's TMU or the DOD equivalent.

In general, Fusion Centers are becoming the focal points for information sharing and will function as an additional layer of review to confirm that the incident warrants treatment as suspicious or potentially connected to terrorism. With the proper training of personnel who perform system management and analytical functions (as discussed elsewhere in this assessment), the use of Fusion Centers as an intermediary should lead to

an effective and standardized vetting process that moves reports quickly through the eGuardian system. There will be vigorous efforts to police eGuardian and eliminate irrelevant, erroneous or otherwise improper reporting. Suspicious activity, incidents and threats that are found to warrant investigation due to a likelihood of having a potential terrorism nexus will be assigned to a member of the FBI's Joint Terrorism Task Forces (JTTFs).

Within the eGuardian system, suspicious activity reports that appear to have a potential nexus to terrorism will be entered by the FBI or a law enforcement partner into the eGuardian system where a record will be created to summarize the nature of the incident for subsequent analytical assessment. The assessment is intended to take place within no more than 30 days and result in one of the following dispositions:

1. DRAFT – threat or report of suspicious activity is reported to the agency reporting space (see Diagram 1a for information flow from Agency Data Input Zone to Fusion Center Management Zone) eGuardian system by an authorized user;

2. REF ERRED – a threat or report of suspicious activity has been referred to the SDR of eGuardian (see Diagram 1a for information flow from Fusion Center Management Zone to eGuardian Exchange Zone) and uploaded to Guardian for further assessment by a FBI/JTTF investigator; or

3. CL OSED – a threat or report of suspicious activity has been reviewed and found to have no nexus to terrorism.

The eGuardian system handles Draft reports in two ways depending on where in the eGuardian workflow the draft exists and how the agency has configured their agency eGuardian workflow. When an agency creates (enters) a suspicious activity report in the eGuardian system, the report is only visible to the eGuardian account holders from that agency. At this point the report is considered to be at agency-level control (see Diagram 1a, Agency Data Input Zone). The report cannot be seen by the Fusion Center responsible for the agency nor can it be seen by the FBI or any other law enforcement agency (LEO eGuardian Special Interest Group). This design enhances privacy protection by restricting access to PII to the agency that created the report. This design function also allows the agency complete control over information they enter into eGuardian.

At the Agency Data Input Zone, the agency reporter or the agency supervisor (if applicable) may elect to retain the information with the eGuardian system pursuant to their agency policy, but for no more than five years. The agency makes the determination whether to share the report by submitting it to their responsible Fusion Center or the TMU, if the agency does not participate in a Fusion Center. The agency may also decide to close the report. If the agency closes the report at the agency level, neither the Fusion Center nor the FBI nor any other agency will ever see the report. If the agency elects to submit the incident to the appropriate Fusion Center, the report continues to remain in draft status and becomes viewable only by the responsible Fusion Center and the FBI. The Draft report is not yet viewable to other law enforcement partners. At the Fusion Center Management Zone (see Diagram 1a), the draft report will be analyzed in an attempt to identify a potential nexus to terrorism.

As noted above, if the Draft report is determined to have no nexus to terrorism, the Draft report will be closed by the Fusion Center and will not be made available for viewing by any other law enforcement partner. Furthermore, closed Draft reports that are determined to have no nexus to terrorism will be deleted from the eGuardian system.

Draft reports in which a threat or report of suspicious activity is indeed found by the appropriate Fusion Center, including the FBI's TMU or DOD equivalent, to have a potential nexus to terrorism are passed to the eGuardian SDR in the eGuardian Exchange Zone and loaded into Guardian. The copy of the report retained in eGuardian will have its status changed from Draft to Referred. At this point the report will be viewable to other law enforcement partners that are members of the LEO eGuardian Special Interest Group. Also, as noted above, if a nexus to terrorism can neither be substantiated nor discounted, the Referred report is determined to be inconclusive, marked as such, and then referred to Guardian for further assessment by the JTTF. Again, at this point, the Referred report will be viewable to other law enforcement agencies with eGuardian accounts. The report will continue to remain in the eGuardian system for tracking and further analytic review. The information in these reports – where a nexus to terrorism is inconclusive or a nexus to terrorism has been substantiated – will be maintained for five years.

This illustrates that the eGuardian workflows heavily restrict information while in "Draft" stage. Reports are only accessible to the eGuardian user community after a potential terrorism nexus is identified or the report is found to be inconclusive in which case the report remains in eGuardian and is referred to Guardian for additional assessment and/or investigation. Likewise, inconclusive reports may later be closed and deleted if, after subsequent analytical evaluation or the passage of time, the report is found to be erroneous, irrelevant or later determined to have no nexus to terrorism.

In addition, in terms of access to the system, the eGuardian user community will consist of only those law enforcement partners who qualify for access to LEO and who are specifically granted access to the eGuardian SIG by TMU.

Other ways that the privacy risk presented by this system is mitigated is through the use of technology. eGuardian will have the ability to conduct data optimization which will identify and eliminate duplicate data objects. This will improve the quality of the data. The system will also be able to provide data segmentation so that disparate rules of SLT law enforcement and federal agencies for limiting collection and access can be implemented. In other words, different rules regarding retention and use that are required by state laws can be incorporated as attributes of the contributed data. Finally, as noted above, the retention period for eGuardian reports generally will be relatively short (5 years) in an effort to balance the need to retain information long enough to discern potential terrorism planning activities but short enough to protect the privacy of individuals whose information is maintained.

Section 3.0
Uses of the System and the Information

3.1 Describe all uses of the information.

eGuardian is first and foremost a reporting system that standardizes existing reporting. Reports will be placed into eGuardian to assist in assessing terrorism-related threats and suspicious activities. In addition, the information derived from the reports that are placed in eGuardian may show links, relationships, and matches among data elements, which will provide the opportunity for analysis and interpretation. The use of the tools in eGuardian will enable analysts, officers, detectives, agents, and other law enforcement investigators to develop leads and identify potential suspects more quickly. Once vetted by a responsible entity, this information will be shared with law enforcement at all levels in order to more effectively identify threats and threat patterns and take actions to mitigate such threats.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

The eGuardian system will contain an analytical functionality to find potential links and patterns between terrorism suspects and suspicious events. Rather than facilitating the search for anomalies based on patterns, however, the point of the system is to collect reports about activities that may be linked to terrorism and then to refer the information for further investigation as necessary and to analyze it for potential linkages that can enhance the ability of the FBI and other law enforcement agencies to take preventative action. There is no capability to use eGuardian for pattern-based data mining as described in section 804 of the Implementing Recommendations of the 9/11 Commission Act of 2007. Should that capability be added and exploited for pattern-based data mining, this assessment will be updated and the activity will be reported to Congress as required by the Act.

3.3 How will the information collected from individuals or derived from the system, including the system itself, be checked for accuracy?

The data will be collected in accordance with procedures established by the respective agencies' policies for collecting data related to suspicious activities that may pertain to terrorism. The information will then be examined by trained investigators for accuracy and authenticity. The system itself will be able to identify duplicate data items and all records will be date and time-stamped. Information that is forwarded to Fusion Centers from SLT law enforcement partners will be subject to additional checks for accuracy and the integrated data available at the Fusion Centers will be utilized to help determine information that is accurate or that is suspect.

3.4 What is the retention period for the data in the system? Has the applicable retention scheduled been approved by the National Archives and Records Administration (NARA)?

e-Guardian has coordinated records retention policies with the FBI's Records Management Division. A determination has been made that information contributed by SLT and other federal agency partners remains under the control of those agencies. The reports that are maintained in the eGuardian SDR are also uploaded to the FBI's Guardian system. The retention schedule for Guardian records will therefore be applied to this information, which will be retained in that system.

As noted earlier, information entered into eGuardian will be characterized in one of three ways: initially, the reported incident will remain in "DRAFT" status until such time as the incident is approved, normally by the responsible entity. While in draft form, the incident is only viewable by the originating agency reporter, and the reporter's supervisor if applicable. If the agency reporter's supervisor decides to share the report outside the originating agency, the supervisor submits the report to the responsible Fusion Center. At this point, the report is only viewable by the reporter, the reporter's supervisor(s), the responsible Fusion Center Administrators and TMU (eFusion Center) personnel. When the incident appears to have a potential nexus to terrorism, upon approval the categorization will change to "REFERRED." Referred indicates the incident has been electronically forwarded, or referred, to the FBI JTTF/Guardian squad for further investigative assessment. If a nexus to terrorism can neither be substantiated nor discounted, the incident remains as "REFERRED," and it will stay in the system for tracking and analytic review. If no nexus to terrorism is established for a particular incident, it will be deleted from the eGuardian system.[4]

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access to eGuardian will be available through a secure interface to Law Enforcement Online (LEO) . LEO, which is a sensitive but unclassified and for authorized use only secure web-based network containing only authorized membership, will provide authentication services for eGuardian users. Each individual LEO user is issued and required to use a login and password that is unique to that user. Passwords must be changed every 90 days. eGuardian will be accessed through a Special Interest Group (SIG) on LEO. Membership in the SIG is by application only and will be drawn only from agencies that have an originating agency identifier (ORI) and thus are recognized law enforcement entities. Membership must also be approved by TMU. In the event an agency with an operational need to share/receive information does not have an ORI, one will be created for that agency by the eGuardian developers/programmers provided appropriate criteria are met. The use of an ORI designation will help to ensure that only those law enforcement personnel who have been cleared for access actually

[4] Information that suggests possible criminal activity may be referred to the appropriate division in the FBI. See section 4.2 below.

have it. Furthermore, members of the SIG will have to agree to a User Agreement each time they log in to eGuardian that dictates how information in the system is to be ingested, maintained and disseminated. The User Agreement will counsel that recorded information should be accurate to the extent possible, timely and relevant to a suspicious activity with a potential nexus to terrorism. Users will be cautioned not to enter information that describes First Amendment protected activities or personal information based solely on ethnicity, race or religion. SIG users' activities while online will be tracked and available for audit so that these rules can be enforced.

Other safeguards to ensure compliance with proper use rules include the limited exposure and non-retention for incidents that do not clear Fusion Center vetting; the retention and deletion controls enforced by the eGuardian system administrator; and the ability to audit and trace user identification if improper use is discovered.

Section 4
Internal Sharing and Disclosure of Information within the System.

4.1 With which internal components of the Department is the information shared?

Other DOJ components, including but not limited to the criminal components of the Department of Justice will be provided access to eGuardian if they have an operational need to know the potential terrorism information that the system contains. To the extent that information is received by TMU that pertains to potential criminal offenses with no apparent nexus to terrorism, and thus it is not appropriate for entry into eGuardian, it may be shared or forwarded to the appropriate division within the FBI or within the Department of Justice for further handling. While the information will not reside in eGuardian, referral of information about potential criminal offenses is consistent with current FBI.

4.2 For each recipient component or office, what information is shared and for what purpose?

Information with a potential nexus to terrorism will be shared with other DOJ components that have an operational need to receive the information.

Some information that is entered into eGuardian may reflect potential criminal conduct, but not conduct that amounts to terrorism. That information will be forwarded to the FBI's Criminal Investigative Division or other responsible law enforcement agency for appropriate disposition. This is not unlike the current situation in which members of the public or law enforcement personnel report incidents that are suspicious or otherwise to an FBI Field Office and the Field Office takes action to mitigate the information – either by forwarding it to the appropriate office for disposition, using it as the basis for additional investigative activity, or closing it as reflecting no violation of law.

4.3 How is the information transmitted or disclosed?

Information will be made available electronically through the eGuardian network or through secure electronic media.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Sharing personally identifiable information carries with it a risk of improper access and/or improper use. The Privacy Act governs the dissemination of information internally within an agency; it is appropriate when there is a need to know. Because other DOJ law enforcement components are expected to be the prime recipients of any data that is shared internally, the internal sharing that is contemplated will meet the Privacy Act requirement. Cookies, which are pieces of text stored on an agency user's computer hard disk, will be used, imbedded in the program, to track access to specific information. Also, only after the incident is approved and REFERRED to Guardian by the Fusion Center is it visible to anyone beyond the original user, the user's immediate supervisor(s), the Fusion Center, and TMU. There is also a risk of data breach from the SIG, but the security features of LEO, coupled with the ability to audit system users, should help mitigate this risk.

Section 5
External Sharing and Disclosure

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Consistent with the National Strategy for Information Sharing, vetted eGuardian information is intended to be shared with other Federal, State, local and tribal law enforcement agencies, including task force members and analytical support personnel.

5.2 What information is shared and for what purpose?

Suspicious activity or threat information having a potential nexus to terrorism will be shared with the goal of creating an efficient, near real-time mechanism for law enforcement at the State, local, tribal and federal level to share and report terrorist threat data and suspicious activity and to discern any otherwise unknown relationships among reported incidents.

5.3 How is the information transmitted or disclosed?

Information is made accessible either through eGuardian, which will be in a SIG on LEO or hard copy information may be printed and disseminated. Section 3.5 describes how information will be accessed in greater detail. The potential also exists for wireless access to the SIG. User agreements will require that information obtained through eGuardian shall not be re-disseminated without approval of a responsible entity or the originating entity.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

By logging onto the SIG, an eGuardian user will be provided a set of behavioral rules, in addition to the standard login disclaimer about the sensitivity of the information, which will describe expectations for use of the information (see attachment 1). In addition, although law enforcement personnel with access to eGuardian are trained officials and understand the rules concerning dissemination of information, additional web-based training of users on the security and privacy requirements of the system as well as system functionality will be provided by LEO. A caveat identifying eGuardian information as Sensitive but Unclassified and For Official Use Only will be included in any dissemination. It is anticipated that these labels will be replaced by a uniform designation as a matter of federal policy; when that policy is fully implemented, the caveat in eGuardian will be amended as required.

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

As noted in the previous answer, Web-based training for all users will be required as part of the eGuardian system.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

All users will have to agree to the User Agreement before being granted access, and caveats about use of eGuardian information will be part of the Agreement. Additionally, the required training for all eGuardian users will cover subsequent use of the information. eGuardian will have the capability to determine who has accessed the system and what data they have created or modified and, thereby, will be able to identify the responsible users if incidents of inappropriate use or disclosure are reported. In addition, periodic audit log reviews will be used to discover access patterns as well as indications of inappropriate access, which will lead to firm controls over users, and can also generate leads to inquire into their use of the data.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Access to eGuardian via LEO is controlled by the LEO network itself. Users obtain access to LEO by applying for and receiving a LEO network login and password, which is only granted to authorized law enforcement agencies. Passwords must be changed every 90 days and any information that is transmitted will meet current security standards. eGuardian will be accessible through a Special Interest Group (SIG). Membership to the eGuardian SIG is by application only. Account holders will be vetted by the applicant's agency. The agency must have an ORI signifying that it is a recognized law enforcement entity. Finally, agencies must apply for membership in the SIG and be approved by TMU. In the event an agency with an operational necessity to share/receive information does not have an ORI, one will be created for that agency by

the eGuardian developers/programmers. This security control should help mitigate the privacy risk that arises from inappropriate access to the data. In further mitigation, audit logs of search transactions will be reviewed every 180 days to check for anomalous activity. TMU will have the ability to delete user accounts at the individual or agency level. Finally, training on using eGuardian will be provided and this training will help ensure that users fully understand the User Agreement concerning dissemination of information. Given the anticipated large number of external users, the risk of misuse of the information or unauthorized access and dissemination of the information by even a trained user always exists. That risk is mitigated significantly by both the restrictions on access to--and dissemination of--unvetted information, as described above, as well as by the audit features noted in Section 5.6 above.

Another privacy risk is that the sum of the data entered into eGuardian may be greater than its component parts, with the result that new and different information about incidents and people alleged to be suspicious becomes apparent. This is, in significant part, the purpose of the system, but it also creates a privacy risk, as well as a risk of public misperception and possible misunderstanding. The privacy risk is that seemingly isolated incidents or observations may lead to more discovery of personal information about individuals in an effort to develop relationships (i.e., "connect the dots") between these and other incidents and observations. This risk is mitigated in part by the inherent nature of the process; i.e., in the end only meaningful relationships that affect national security will be developed and acted upon. The incidents or observations containing personal information that remain isolated or the relationships among incidents that do not develop investigative value will not lead to further action and will be retained in eGuardian for the limited time indicated above. These on-going vetting and analytical processes should minimize the risk of unwarranted and inappropriate dissemination of irrelevant personal information.

Section 6.0
Notice

6.1 Was any form of notice provided to the individual prior to collection of information? (If yes, please provide a copy of the notice as an appendix. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

General notice concerning the FBI's collection, use and maintenance of law enforcement and intelligence information is provided through the System of Records Notice for the Central Records System (63 Fed. Reg. 8671). As noted above, that notice describes the fact that the FBI maintains computerized investigative information extracted from its own files or those of other governmental sources. Because the collection of eGuardian information may be done in connection with law enforcement activities, no individual notice will be given.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

eGuardian suspicious activity reports, in many cases, will originate from observations made by law enforcement officers and from information received from the general public. In those situations, no opportunity or right to decline information is provided. The reports that are submitted are nevertheless vetted by trained law enforcement personnel and funneled through a second review at a Fusion Center or comparable entity before being added to the system.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Because of the nature of the records at issue, the opportunity to consent to particular uses of the information is not provided.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The privacy risk associated with eGuardian is the lack of notice that information about individuals is being collected, used and maintained. The FBI has published a Privacy Act System of Records Notice (SORN) for FBI's investigative records, which provides general notice regarding entities with which and situations when the FBI may share investigative records, and a separate system notice for eGuardian will be published to provide further transparency. The FBI's routine uses for its systems and its Blanket Routine Uses provide further notice of the ways in which information collected by the FBI is shared. These notices, therefore, mitigate the privacy risk. No individual notice is provided, however, because the information in this system is collected by law enforcement and personal notice is not feasible.

Section 7.0
Individual Access and Redress

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Applicable regulations found in 28 CFR Part 16, Subparts A and D, which have been issued pursuant to the Freedom of Information and Privacy Acts, govern requests for access to information in FBI files. To the extent that other federal agencies, which contribute information to eGuardian, have processes in place to govern access or redress, those processes will apply to the information contributed by these agencies. As entries into eGuardian will most often be made by state and local law enforcement officers, the information may be retained in state and local agency records as well. Access to and opportunity to seek redress for those records is controlled by state law and procedures.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

28 C.F.R. 16.41 and 16.46 provide information on individual access and amendment of FBI records. Amendment of FBI records is a matter of discretion as the records are exempt from the Privacy Act amendment provisions.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual.

See previous response.

7.4. Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

Redress is generally not available except to the extent described in Section 7.2, above, but eGuardian is not intended to be a data repository, but a dynamic system where corrections and updates will be made as necessary during the short process of ascertaining whether a particular report merits further investigation because of a potential nexus to terrorism. If no nexus to terrorism is found, the SAR will be deleted from the system.

As a general matter, although FBI records are exempt from Privacy Act access and amendment procedures, the FBI strives to maintain accurate information and will, in its discretion, consider amendment requests.

Section 8.0
Technical Access and Security

8.1 Which user group(s) will have access to the system?

eGuardian access will be provided to State, local, and tribal law enforcement officers and agencies that have a law enforcement mission need for suspicious activity reports. Other federal law enforcement entities, including Department of Justice components, DHS and DoD entities with law enforcement missions, including force protection, will be provided access.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contractors will have access to the system in order to perform system maintenance and administration. In addition, to the extent contractors are assigned to any of the agencies that will have access to eGuardian, these individuals will also, upon proper vetting and clearances, be able to access the system.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes. eGuardian will have the following user roles:

1. Police Officer/Investigator/Intelligence Analyst/Support Contractor. These roles are generally reserved for individuals who create eGuardian incidents and are responsible for investigating and/or conducting analysis of terrorist-related threats and suspicious activity reports entered into the system. This role may include, at the discretion of the agency, an agency eGuardian supervisor who will control all eGuardian report dissemination from their agency. All such work will be electronically submitted to a coordinator at a responsible entity for review and authorization to be submitted into Guardian.

2. Coordinator/Administrator: The individual(s) assigned to this role works within the responsible entity to evaluate the information in eGuardian and performs other administrative functions with respect to the system. Individuals with this role have the ability to refer incidents to Guardian.

3. TMU will have overall administrative oversight of eGuardian and the capacity to monitor user roles assigned to each participating agency. Responsible entities will also exercise administrative oversight of users at their locations. With each participating agency, however, the determination of roles will be made locally.

8.4 What procedures are in place to determine which users may access the system and are they documented?

eGuardian will have restricted access and will follow a process regulated by TMU and by LEO. Prospective users must first clear the vetting requirements imposed by the LEO network, which include demonstrating that a proposed user is a member of an authorized law enforcement agency that is assigned an ORI or an agency with an operational necessity to share/receive information. In the event an agency with an operational necessity does not have an ORI, one will be created for that agency by the eGuardian developers/programmers, if appropriate. LEO revalidates all users' agency affiliation twice a year. Additionally, access to the eGuardian SIG will be controlled by TMU, which must approve all users. The procedures for system access are documented in policy and procedure documents developed by TMU for the eGuardian system.

8.5 How are the actual assignments of roles and rules verified, according to established security and auditing procedures?

Individual member agencies will be able to structure user roles and customize the work flow to fit their own needs. The responsible entities, however, will exercise administrative oversight of the system, which will include auditing for appropriate system access and use.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Each user will have an individual account that requires a login and password for LEO. These accounts will be auditable. Each responsible entity, moreover, will have the responsibility to audit their users and will be obligated to report suspected misuse and security compromise. Rules of Behavior and training will cover the appropriate use of data and the penalties for misusing the information.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

As indicated previously, web-based training will be available to the user to assist with system access and procedure. In addition, eGuardian administrators from responsible entities will be provided classroom training that will emphasize their roles and responsibilities. A privacy statement will also be contained in the user agreement electronically signed by each participating agency.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification and Accreditation last completed?

The Certification and Accreditation of the system is expected to be completed in early July and an Authority to Operate will be issued at that time.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and how were they mitigated?

Privacy risks from this type of system stem from improper access and inadequate security. These risks have been mitigated in several ways. eGuardian access is based on role and function. In order to access the system, users must be sworn law enforcement officers or support personnel assigned to perform law enforcement analysis and/or criminal intelligence, as evidenced by an ORI. All users are vetted through LEO before they are permitted entry into the eGuardian Special Interest Group. Web-based training will be available to the user to assist with system access and procedures and the use of the information contained therein, with emphasis on privacy controls. Once an individual is vetted and authenticated through LEO, and then granted access to the eGuardian SIG, the individual's web-based session is controlled with computer software and hardware components secured behind accredited FBI security infrastructure. Placing eGuardian behind the FBI firewall and under the oversight of TMU will improve the security posture of the system.

Section 9.0
Technology

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Yes. Several systems were reviewed and evaluated including an in-house solution. Final system design was based on operational imperatives and privacy and security attributes.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Data integrity, privacy and security were important considerations in the development of this system. The task was to develop a robust information sharing system that would serve the needs of users for timely, relevant and accurate information in a secure environment while protecting privacy and ensuring data integrity and security. The system is designed to help investigators become aware of and make connections between reports of suspicious activities and terrorism threats in order to improve the security posture of the United States. Operationally the goal is to either close or refer for enhanced investigation all leads within a short period of time.

eGuardian is built upon and incorporates the lessons learned from the Guardian system and is designed to seamlessly interface with it. To enhance privacy protections for information that is added by SLT law enforcement personnel, a decision was made to use Fusion Centers as initial vetting points, as these groups can bring to bear enhanced information availability to ensure that suspicious activity reports and reports of incidents that have a potential nexus to terrorism meet a required threshold for system inclusion. TMU and a DOD fusion-like center will perform the same type of "fusion" for reports from federal entities. System functionality is designed to permit contributors to modify their entries as new information is received, and the need to check the system for updates will be incorporated as part of the required training for all users.

The eGuardian system was placed on an FBI server to enhance security and membership in the Special Interest Group of eGuardian users will be vetted through LEO, which performs this function for a variety of other law enforcement entities. User access will also be audited by TMU personnel.

9.3 What design choices were made to enhance privacy?

The eGuardian system is set up so that participating agencies can restrict the information they contribute in order to deny access to certain groups or individuals. This choice takes into account various state laws which have differing privacy requirements for sharing information and also allows contributors more control over their own information. A decision was also made to control access to reports in eGuardian to sworn law enforcement and analytical support personnel in order to ensure that those with training in handling sensitive law enforcement and terrorism-related information are the only ones who can access the system. The decision was made to use LEO as the hosting organization because it is an FBI-owned, web-based, sensitive but unclassified network

that provides controlled access to facilitate information sharing. Placement of eGuardian on the Internet allows for ease of use but potentially exposes personally identifiable information to outside attack. LEO provides a restricted and more secure access to this information, which will enhance both privacy and security.

The work flow was created with privacy in mind so that contributors can easily update their information or mark it with a commentary to let other viewers know of particular issues pertaining to data integrity or privacy. Any re-dissemination of information will be subject to permission controls of the responsible or originating entity.

Conclusion

The eGuardian threat tracking system supports the FBI mission to prevent terrorist attacks on the United States. It is designed to mitigate and vet all threats and suspicious activities with a potential nexus to terrorism and assure they are properly addressed and available for trend analysis. Establishing an electronic system that will allow SLT and federal law enforcement partners to enter terrorist threat information and suspicious activity reports with a possible nexus to terrorism and share it with each other will facilitate the type of information sharing envisioned in the National Strategy for Information Sharing.

eGuardian has been designed in consultation with legal, privacy and security personnel in the FBI and elsewhere in order to ensure that privacy protections and security controls are integrated into system development and functionality. This privacy impact assessment is part of the process of ensuring that the system accounts for privacy concerns while creating an electronic environment that will facilitate operational imperatives.

Responsible Officials:

/s/ 11/25/08

Gerald J. Rogero, III — Date
FBI Program Manager
Threat Monitoring Unit (TMU)
Federal Bureau of Investigation
571-280-6372

/s/ 11/25/08

Christopher Light — Date
FBI System Developer
Foreign Terrorist Tracking Task Force (FTTTF)
Federal Bureau of Investigation
703-682-4662

/s/ 11/25/08

David C. Larson — Date
Chief Privacy and Civil Liberties Officer
Federal Bureau of Investigation

/s/ 11/25/08

Vance E. Hitch — Date
Chief Information Officer
Department of Justice

/s/ 11/25/2008

Kenneth P. Mortensen — Date
Acting Chief Privacy and Civil Liberties Officer
Department of Justice

Attachment 1

eGuardian User Agreement

Contact your local Joint Terrorism Task Force (JTTF) immediately by phone for any urgent matters with a potential nexus to terrorism.

eGuardian is a sensitive but unclassified system for official use only. Information classified CONFIDENTIAL and above cannot be placed into eGuardian under any circumstances. This includes all information that is SECRET, TOP SECRET OR COMPARTMENTED. Neither FISA-derived information nor Grand Jury 6(e) material nor any other information that is legally restricted may be placed into eGuardian.

The suspicious activities contained in eGuardian may be raw and unvetted data. "Suspicious activity is defined by the Program Manager of the Information Sharing Environment (PM/ISE) as observed behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal or other illicit intention. Suspicious activities may include, but are not limited to, surveillance, cyber attacks, probing of security and photography of key infrastructures and facilities. Do not conduct any unilateral investigation with any reported incident without the coordination of the originating agency/author. Do not arrest any individual based solely on the information in eGuardian unless there is evidence of a violation of State, Local or Federal statutes.

By signing the user agreement, the parties will agree to the Fusion Center and TMU policy that sets forth the mission, goals, functions, management, principles, membership, staffing, information sharing policies and protocols and privacy and security attributes of the eGuardian system.

Membership in the SIG is by application only and will be drawn only from agencies that have an originating agency identifier (ORI) and thus are recognized law enforcement entities.

No entry into eGuardian may be made based solely on the ethnicity, race or religion of an individual or solely on the exercise of rights guaranteed by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States.

If you determine that information you have previously submitted is erroneous, you are responsible for updating or correcting the information in eGuardian. If you discover information that has been contributed that you know is erroneous, you should notify the submitter so that the information can be corrected.

Proceeding to the eGuardian Threat Tracking System indicates you have been informed of, agree to, and will abide by these restrictions. Incidents not meeting the criteria of suspicious activities or with a potential nexus to terrorism and that, further, do not comply with the above-stated rules, will be immediately deleted from eGuardian. Furthermore, by clicking on the User Agreement check box, you agree to the policies that govern the eGuardian system. For further information about the eGuardian policy, please return to the policy link on the LEO eGuardian member area page.

Information obtained through eGuardian shall not be re-disseminated without the approval of a responsible entity or the originating entity.

The TMU will conduct periodic audits of the system to ensure that the rules are followed. Failure to comply with this agreement will result in the termination of your eGuardian membership.