*e*Guardian

Frequently Asked Questions

eGuardian is a secure, 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 and the Federal Bureau of Investigation (FBI) Joint Terrorism Task Forces (JTTFs).

1. **How do the eGuardian and Guardian threat tracking programs differ?**

eGuardian

- Available to users via Law Enforcement Online (LEO)
- System designed to share potential terrorist threats, terrorist events, and suspicious activity information at the Unclassified Law Enforcement Sensitive level

Guardian

- Available to users with access to FBInet
- System designed to share potential terrorist threats, terrorist events, and suspicious activity information up to the Secret level

When an incident is approved in the eGuardian unclassified system, the incident is uploaded simultaneously to Guardian and eGuardian. Both systems have a link to the FBI JTTFs.

2. **How does eGuardian differ from other threat databases?**

- eGuardian is the only threat tracking system that shares potential terrorist threats, terrorist events, and suspicious activity information with state, local, tribal, and federal law enforcement agencies; state fusion centers; and your local FBI JTTF
- eGuardian is the only system that allows law enforcement partners to access unclassified data from Guardian

3. **What features does eGuardian offer?**

- eGuardian provides a near real-time information sharing environment
- In addition to the potential threats, terrorist events, and suspicious activity information, eGuardian offers the ability to attach documents, images, videos, and audios
- eGuardian hosts geospatial mapping, live chat, and link analysis capabilities
- The eGuardian Special Interest Group (SIG) is moderated by FBI personnel assigned to the Threat Monitoring Unit through FBI Headquarters (HQ)
- The eGuardian database is searchable using advanced query techniques

4. **How does eGuardian benefit me?**

- Free to all law enforcement
- Import and export capabilities to create statistics and charts
- A simple, secure Web interface accessible through LEO
- Access to a consolidated, global database of terrorist-related incidents
- Cobranding of the Web site and documents
- Flexible work flow and data segmentation
- Easy access to consolidated contact information

5. **How do I access or input information into eGuardian?**

- Access to eGuardian is available through the eGuardian SIG hosted via LEO
- Once your account has been validated, you will be able to access eGuardian information from any computer with Internet access
- eGuardian provides an intuitive, user-friendly interface for entering and viewing potential terrorist threats, terrorist events, and suspicious activity information

6. **Will all users have the ability to enter an incident?**
    - Access to the eGuardian SIG will be determined by eGuardian SIG moderators in conjunction with your local fusion center
    - eGuardian is designed for use by law enforcement/intelligence analysts with an operational need

7. **Where does the data go after it is entered?**
    - Once an incident has been created, it will be submitted for review to the local fusion center or the eFusion center, which will refer incidents to the system
    - Once the incident has been referred, it will be uploaded into both Guardian and eGuardian, where it will be made available to all eGuardian and Guardian users

8. **Who owns the information in eGuardian, and how long will it remain in the system?**
    - The originating agency will be the owner of its own information
    - During incident input, the agency will select a retention date from a drop-down menu
    - Information that passes to Guardian will remain in eGuardian and include a tracking number and contact information for the assigned FBI field division
    - Information that is deemed inconclusive will remain in eGuardian for a maximum of five years in accordance with 28 Code of Federal Regulations (CFR) Part 23

9. **Will the agencies and departments represented on the National Joint Terrorism Task Force (NJTTF) have access to eGuardian?**
    - Yes. The FBI HQ Threat Monitoring Unit will be the approving authority. Access for nonsworn law enforcement and intelligence analysts may be limited to fusion centers, JTTFs, NJTTF, and agencies with an operational need

10. **Will I have to enter several passwords to access eGuardian?**
    - No. You only need to enter your LEO password
    - Once logged in to LEO, you are connected to the eGuardian SIG via a quick link and, after agreeing to a disclaimer, directed to the eGuardian system

11. **How long will it take to get information into eGuardian?**
    - Once an incident has been created in eGuardian, it will be transmitted to the fusion center for review
    - A timely review will lead to rapid transmission to the JTTF and Guardian

12. **Who else can view the incident once it has been created, and how do I track it?**
    - Once an incident is accepted into eGuardian, anyone with LEO access and validation for the eGuardian SIG will be able to view the incident
    - A review of the incident in eGuardian will reveal the status of the incident and contact information for the coordinating FBI field division

13. **Initial Project**
    - A phased rollout to the law enforcement community is slated to begin in December 2008
    - For further updates on eGuardian, please check the eGuardian SIG hosted by LEO
    - Feel free to post questions on the E-GUARD Forum on LEO