eGuardian *and the* Nationwide SAR Initiative

*Law Enforcement's **Free** Online Information Sharing Tool*

What is eGuardian?

The eGuardian system was developed by the Federal Bureau of Investigation (FBI) in **2008** to help meet the challenges of collecting and sharing terrorism-related activities among law enforcement agencies across various jurisdictions as outlined in the **2007** White House National Strategy for Information Sharing.

The system is:

- An incident reporting system that standardizes existing reporting types;
- The primary shared data repository for suspicious activity reporting (SAR);
- Hosted through the Law Enforcement Enterprise Portal (LEEP), a sensitive but unclassified (SBU) web-based network.

What does eGuardian do?

- Facilitates SAR covering five FBI program types: counterterrorism, cyber, weapons of mass destruction, criminal, and counterintelligence. Reports can involve suspicious observed terrorism-related behavior, as defined by the Nationwide SAR Initiative, or suspected criminal activity, including potential threats to national security.
- The mapping and search features facilitate pattern and trend analysis of incident data.

eGuardian User Criteria

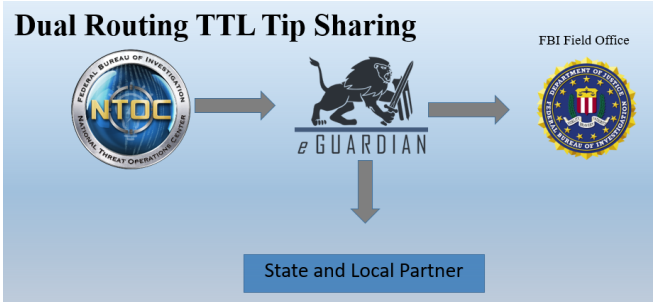
Access is restricted to US citizens with a need to know who meet one of the following criteria:

- Federal, state, local, tribal, and territorial law enforcement agencies and the Department of Defense (FSLTT/DOD) across the nation and at U.S. military and government installations around the world, including:
  - More than **8,700** law enforcement and homeland security professionals
  - Over **2,200** member organizations
  - **80** state and major urban area fusion centers
- Sworn law enforcement
- Personnel working in direct support of law enforcement
- Force protection personnel

How is SAR used?

SAR is migrated to the FBI's internal Guardian system, where it is **assigned** to the appropriate **Joint Terrorism Task Force (JTTF) or FBI field office for further investigative action as warranted.**

- The FBI uses eGuardian to directly transmit nonfederal **Threat-to-Life incidents** to partnering agencies while providing field offices notification of the same incidents in Guardian for awareness and information only. The FBI also uses eGuardian to **share incident information from Guardian**.



Why use eGuardian?

- **Free:** **No cost** to FSLTT/DOD agencies
- **Ease:** Interface is comprehensive, easy to use, and dynamic. The FBI Criminal Justice Information Services Division (CJISD) and Information Technology Applications and Data Division (ITADD) continue to deploy system enhancements to increase the visibility and usability of eGuardian for partner agencies
- **Training:** eGuardian training is site accessible through LEEP; additional training is provided through Justice Connect and links within eGuardian
- **Data:** Over **140,000** incidents in the past five years
- **Collaboration:** Users can add notes to existing incidents
- **Searches:** Advanced capabilities and subscriptions
- **Control:** Agencies can limit or share their incidents with other users, promoting information sharing and awareness
- **Accessibility:** Accessible from virtually any internet-connected device
- **Manageable:** Utilizes a single sign-on with LEEP

Need Access

For eGuardian access, follow these steps:

- Obtain access to the LEEP or a LEEP-partnered identity provider.
- To apply for LEEP access, go to https://www.cjis.gov and select "Apply for an Account."
- Once logged into LEEP, locate and click on the eGuardian icon in the list of available services.

The Nationwide SAR Initiative (NSI)

NSI Overview

The Nationwide SAR Initiative (NSI) establishes standardized processes and policies that provide the capability for FSLTT, campus, and railroad law enforcement and homeland security agencies to share timely, relevant terrorism-related suspicious activity reports, or ISE-SARs, through a distributed information sharing system that protects privacy, civil rights, and civil liberties (P/CRCL). This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing ISE-SAR information.

Technical Assistance

- DHS offers technical assistance services that enable the NSI to coordinate with FLSTT, fusion center partners, and the eGuardian system to provide ad-hoc services that enable partners to achieve their SAR program goals.
- The NSI further conducts periodic trainings to help fusion centers proficiently access eGuardian, adjudicates authorization permissions for receipt and dissemination of ISE-SAR, and provides hands-on utilization of the eGuardian search tool.

Privacy

- The protection of P/CRCL is paramount to the success of the NSI.
- The NSI requires each fusion center to consider privacy throughout the SAR process by fully adopting a practical framework that enhances the fidelity and quality of reporting output; it also emphasizes the importance of P/CRCL compliance as an essential best practice.
- NSI stakeholders are strongly advised to perform P/CRCL impact assessments to be successful in identifying privacy risks and vulnerabilities within their institutional SAR programs.

Training

- DHS has designed a training strategy for the NSI that is intended to increase the effectiveness of FSLTT law enforcement and homeland security partners in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to identify and prevent acts of terrorism.
- The training is broken down into focus areas for frontline law enforcement officers, analysts, executives, and hometown partners, with each training focusing on the respective level of responsibilities and duties of various law enforcement and homeland security partners.
- You can access both the NSI-SAR and SAR Fundamentals eLearning training courses at: https://www.dhs.gov/nationwide-sar-initiative-nsi/online-sar-training.

Contact Information

FBI eGuardian: HQ-DIV26-eGUARDIAN-HELPDESK@fbi.gov
DHS National Threat Evaluation Reporting (NTER) — NSI Program Management Office: NTER.NSI@hq.dhs.gov