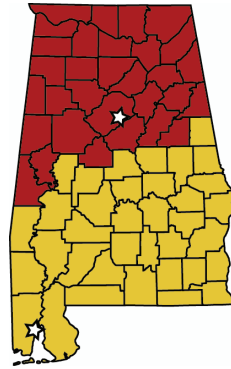


Secure Homeland Access and Reporting Environment

- ★ The U.S. Department of Homeland Security (DHS) funded the development of the Secure Homeland Access and Reporting Environment (SHARE), a program developed to demonstrate effective reporting of potential terrorism events through diverse technologies.
- ★ This program is part of DHS's Information Technology Evaluation Program (ITEP).
- ★ A primary goal of SHARE is to establish a link between State/Federal homeland security officials and *field officers, including private sector security officers*.
- ★ The **Terrorist Incident Reporting Portal** is part of SHARE and was developed to provide private sector security officers with a mechanism to easily report threat information.
- ★ Reports submitted though SHARE are compiled and analyzed by members of the Alabama Intelligence Analysis Cell (IAC).
- ★ IAC includes personnel from the FBI, the U.S. Attorney's Office (USAO), the U.S. Department of Homeland Security (DHS), and several state and local agencies, including the Alabama Bureau of Investigation (ABI).

REPORT ALL EMERGENCY INCIDENTS



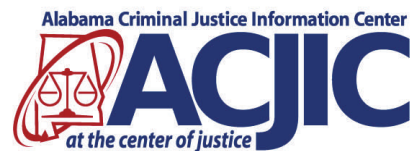
FBI North Alabama
Birmingham
205-326-6166

FBI South Alabama
Mobile
251-438-3674

*Private Sector Security Supervisors are encouraged to report **all** potential terrorism-related incidents, no matter how seemingly insignificant, through the SHARE system. Go to:*

<https://push.alacop.gov>

For more information, contact:



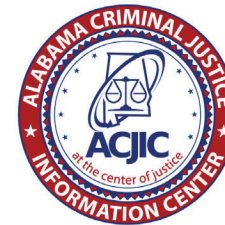
770 Washington Avenue, Suite 350
Montgomery, Alabama 36130
(334) 242-4900

PUSH

<https://push.alacop.gov>



Private Sector Security Terrorism Incident Reporting Portal



A collaborative effort of
Federal, State and Local Law Enforcement
and the Private Sector



PROTECTING ALABAMA CITIZENS TOGETHER

What is the Terrorism Incident Reporting Portal?

The PUSH Terrorism Incident Reporting Portal is an online portal environment that provides **private sector security officers** with a secure capability to report potential terrorism-related incidents. The portal also provides important resources, such as daily security updates from DHS, research tools, and directories of resources.

The Reporting Portal uses Internet

technology and provides an easy to use data collection wizard to prompt the user for pertinent information.

The **reporting tool** has the following sections:

General:

Identification on the individual reporting the incident and the person who observed the incident (if different).

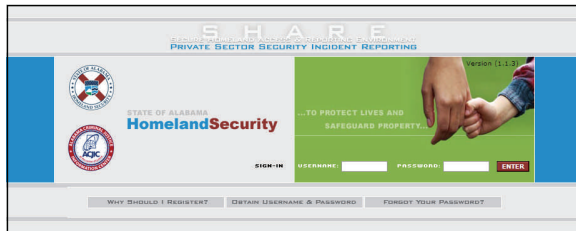
Who: Details on the person(s) involved in the incident.

What: A number of data elements to classify the incident.

When: The time or time range of the event.

Where: The location of the target and/or the place that the incident occurred.

Narrative: Description of the observed activity not already recorded on the form.



Additional PUSH Portal Features

- Critical Infrastructure Directory
- Emergency Response Directory
- Emergency Plan Center (with sample plans)
- Research Tools
- USDHS Daily Open Source Updates

What activity should be reported?

The following are examples of the types of suspicious activities that should be reported. Do not hesitate, though, to report any activity that seems to be unusual.

- ✓ Unusual or prolonged interest in security measures or personnel
- ✓ Unusual behavior such as staring or quickly looking away from personnel or vehicles entering or leaving designated facilities
- ✓ Observation of security reaction drills or procedures
- ✓ Loitering near restricted areas or sensitive sites
- ✓ Use of multiple sets of clothing and identification

✓ Approaching security checkpoints with unusual requests such as asking for obscure directions

✓ Attempting to make unscheduled deliveries or “complimentary” maintenance visits

✓ Attempts to purchase or steal facility blueprints

✓ Increase in anonymous telephone or email threats to facilities

✓ Prolonged static surveillance using operatives disguised, as panhandlers, shoe shiners, food or flower vendors, not previously seen in the area

- ✓ Discreet use of still cameras, video recorders or note taking or sketching material
- ✓ Suspicious or improper attempts to acquire official vehicles, uniforms, badges, access card or identification for key facilities
- ✓ Attempts to gain sensitive information regarding key faculties or personnel through personal contact or by telephone, mail or email
- ✓ Attempts to penetrate or test physical security and response procedures
- ✓ Attempts to improperly acquire explosives, weapons, ammunition, dangerous chemicals, etc.
- ✓ Presence of individuals who do not appear to belong in the workplace
- ✓ Wearing inappropriate attire such as loose or bulky clothing inconsistent with weather conditions

✓ Protruding bulges or exposed wires under clothing

✓ Theft or purchase, particularly with cash of large delivery vehicles, cans, cargo containers, etc.

✓ Drivers who operate the vehicle in an overly cautious manner, attempt to abandon the vehicle or seem overly cautious about accessing the cargo area

✓ Incidents involving ramming or bumping of physical security barriers or the unauthorized parking of vehicles on or near a facility