Critical Infrastructure Protection and Suspicious Activity Reporting

Texas Department of Public Safety
Intelligence & Counterterrorism Division
Texas Homeland Security Strategic Plan

• **GOAL:** Prevent terrorist attacks in Texas and prevent criminal enterprises from operating successfully in Texas

  – **OBJECTIVE:** Expand and enhance the statewide intelligence capability that reduces the threat of terrorism

    • **ACTIONS:**
      - Expand and enhance multi-agency, multi-jurisdictional fusion capabilities throughout the state
      - Employ the Texas Fusion Center and regional fusion centers to integrate homeland security-related information and intelligence across all agencies, jurisdictions and disciplines in Texas
      - Enlist the homeland security community, including health services, agriculture, animal health, private sector, and other critical infrastructure stakeholders, as collectors and consumers of intelligence

FOR OFFICIAL USE ONLY
Goal: Protect the state’s Critical Infrastructure and Key Resources (CIKR) in support of the National Infrastructure Protection Plan.

- Develop Texas Infrastructure Protection Plan (TIPP) and appropriate Sector-Specific Plans.
- Coordinate with DHS, State Agencies, Local Governments, and the Private Sector to identify, validate, and update CIKR data within the State of Texas and develop appropriate strategies for protection and resiliency.
- Engage private sector partners through the Private Sector Advisory Council (PSAC) to implement CIKR protection.
- Advise the Governor or his/her designee on homeland security related issues pertaining to CIKR.
- Evaluate and assess threats, vulnerabilities and risks related to CIKR.
Physical Security & Cyber Security

- All-threat risk & vulnerability assessments
- Information sharing
- Understand system vulnerabilities and interdependencies
- Suspicious activity reporting
- Trend analysis
- Incorporate industry needs into strategy
- Strategic level planning
- Champion activities to protect dam infrastructure and promote resilience
What is HSIN Texas Infrastructure Protection (HSIN-TIP)?

HSIN Texas Infrastructure Protection (HSIN-TIP) is a web-based, Sensitive But Unclassified (SBU) information sharing platform intended to connect all Infrastructure Protection mission partners in the State of Texas.

**HSIN-TIP:**

- Improves situational awareness.
- Facilitates collaboration between public and private sectors.
- Connects partners to both State-centric and nationwide Infrastructure Protection resources.
- Connects users to HSIN-CS where they can get Sector-specific CIP information from a National perspective.
HSIN-CS Dam Community of Interest

- HSIN National Dam Community of Interest
- Tools/Resources
  - SAR Reports
  - Patriot Reports
  - Intel Bulletins
  - Cybersecurity
  - Reference Library
  - Discussion Forum
Threat Liaison Officer Program (In Development)

- Statewide All Threats Enterprise
  - Austin Regional Intelligence Center
  - Dallas PD Fusion Center (MOSAIC)
  - El Paso PD Fusion Center (MATRIX)
  - Houston Regional Intelligence Service Center
  - North Central Texas Fusion Center
  - Southwest Texas Fusion Center
  - Texas Fusion Center

- A Threat Liaison Officer (TLO) is anyone working closely within the public safety/homeland security community who has been through an approved fusion center liaison officer training
• Program will provide participants an effective means of sharing information related to local and regional criminal threats, suspicious activity, and large scale incidents.

• This program will integrate participants into a statewide system of resources through a process of combining local fire and law enforcement agencies, emergency management, federal and state partners, and key private organizations into an effective and sustainable two-way flow of information.
Facilitate the exchange of information between TxFAC and stakeholders within our area of responsibility

Benefits of a robust, multidisciplinary TLO program

- Improve the quality and efficiency of information exchange between TxFAC, local first responder communities and national level intelligence/law enforcement agencies
- Increase awareness of terrorism and criminal indicators, in accordance with applicable privacy and civil rights/civil liberties
- Increase opportunities to detect, deter, and prevent crime and terrorist threats
- Increase participation in TxFAC activities for non-law enforcement partners
- Develop a network of subject-matter experts (SME)
Suspicious Activity Report

- Participants in Nationwide SAR Initiative
- Methods of Reporting
  - Community Member
  - Private Sector
  - INT-7 Field Interview Card
  - Law Enforcement
- Future of SARs
  - Automate THP Reporting
  - Integrate into analytical process
  - Geospatial Mapping
  - Statewide All Threats Enterprise

(Austin Regional Intelligence Center, Dallas PD Fusion Center (MOSAIC), El Paso PD Fusion Center (MATRIX), Houston Regional Intelligence Service Center, North Central Texas Fusion Center, Southwest Texas Fusion Center, Texas Fusion Center)

www.iwatchTX.org

FOR OFFICIAL USE ONLY
Benefits of TrapWire in the Fusion Center

• Access to a predictive analysis system designed to detect patterns of terrorist pre-attack surveillance and logistical planning before an attack

• Unique capacity to compare suspicious activity reporting with other major threat areas in America and abroad, to include Los Angeles, Las Vegas, London, and New York for greater situational awareness and information sharing

• A training program which will allow fusion center personnel to be better prepared to collect, analyze and interpret suspicious activity. This enhanced capability will allow TxCFC personnel to better detect warning of pending attack/threat and notify the appropriate officials in order to prevent major crimes and acts of terrorism

• An interactive and intuitive on-line reporting method for community members (public) and other collectors (LE – Private Sector) to report suspicious activity to TxCFC
## Suspicious Activity Reporting: Indicators and Behaviors

<table>
<thead>
<tr>
<th>Behaviors</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Potential Criminal or Noncriminal Activities Requiring Additional Information During Investigations</strong></td>
<td></td>
</tr>
<tr>
<td>Eliciting Information</td>
<td>Questioning individuals at a level beyond mere curiosity about particular facets of a facility’s or building’s purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.</td>
</tr>
<tr>
<td>Testing of Security</td>
<td>Interactions with or challenges to installations, personnel, or systems that reveal physical personnel or cybersecurity capabilities.</td>
</tr>
<tr>
<td>Recruiting</td>
<td>Building operations teams and contacts, personnel data, banking data, or travel data.</td>
</tr>
<tr>
<td>Photography</td>
<td>Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc. All reporting on photography should be done within the totality of the circumstances.</td>
</tr>
<tr>
<td>Observation/Surveillance</td>
<td>Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.</td>
</tr>
<tr>
<td>Material Acquisition/Storage</td>
<td>Acquisition of unusual quantities of percursor materials such as cell phones, pagers, fuel, and timers, such that a reasonable person would suspect possible criminal activity.</td>
</tr>
<tr>
<td>Acquisition of Expertise</td>
<td>Attempts to obtain or conduct training in security concepts (military weapons or tactics) or other unusual capabilities that would arouse suspicion in a reasonable person.</td>
</tr>
<tr>
<td>Weapons Discovery</td>
<td>Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.</td>
</tr>
<tr>
<td>Sector-Specific Incident</td>
<td>Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector) with regard to their personnel, facilities, systems, or functions</td>
</tr>
<tr>
<td><strong>Defined Criminal Activity and Potential Terrorism Nexus Activity</strong></td>
<td></td>
</tr>
<tr>
<td>Breach/Attempted Intrusion</td>
<td>Unauthorized personnel attempting to enter or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g., police/security, janitor).</td>
</tr>
<tr>
<td>Misrepresentation</td>
<td>Presenting false or misusing insignia, documents, and/or identification to misrepresent one’s affiliation to cover possible illicit activity.</td>
</tr>
<tr>
<td>Theft/Loss/Diversion</td>
<td>Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents [classified or unclassified] which are proprietary to the facility).</td>
</tr>
<tr>
<td>Sabotage/Tampering/Vandalism</td>
<td>Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.</td>
</tr>
<tr>
<td>Cyberattack</td>
<td>Compromising or attempting to compromise or disrupt an organization’s information technology infrastructure.</td>
</tr>
<tr>
<td>Expessed or Implied Threat</td>
<td>Communicating a spoken or written threat to damage or compromise a facility/infrastructure.</td>
</tr>
<tr>
<td>Aviation Activity</td>
<td>Operation of an aircraft in a manner that reasonably may be interpreted as suspicious or posing a threat to people or property. May or may not be in violation of Federal Aviation Regulations.</td>
</tr>
</tbody>
</table>
• **What information should be included when documenting a suspicious activity?**

It is important to include all information obtained so that the full context of the incident is apparent to anyone who reviews the report. This includes detailed descriptions of people, vehicles, facilities, etc. It is also important to include your or complainant’s information (name, phone number, etc.) if available.

• **When completing a suspicious activity report (SAR), individuals must remember the following:**
  - The information for the SAR must be legally obtained
  - The information submitted must be relevant to the identification of the subject or the subject’s criminal conduct or activity.
  - The information gathered cannot be based solely on the political, religious, or social views, associations, or activities of any individual or any group.
Suspicious Activity Report

Online SAR Training for Law Enforcement and Hometown Security Partners

The NSI training strategy is a multifaceted approach designed to increase the effectiveness of state, local, and tribal law enforcement and public safety professionals and other frontline partners in identifying, reporting, evaluating, and sharing pre-incident terrorism indicators to prevent acts of terrorism. To increase the effectiveness of this multifaceted approach, the NSI has developed training programs for frontline officers and hometown security partners regarding documented and verified behaviors and indicators that, when viewed in the totality of circumstances, may indicate terrorism-related criminal activity. Both the SAR Line Officer Training and each sector-specific SAR Hometown Security Partners Training discuss how to report identified suspicious activity to the proper authorities while maintaining the protection of citizens' privacy, civil rights, and civil liberties.
Bidirectional Information Sharing

PRIORITY CRIME REPORT

LAW ENFORCEMENT

PRIVATE SECTOR

Suspicious Activity Reports

LAW ENFORCEMENT

PRIVATE SECTOR

Information authorized by law on local crime trends, modus operandi, incident reports, threat assessments

SAR Summary:

Two subjects posing as members of the Cherokee Nation have been targeting local power plants. They are very convincing and are even dressed in Native American attire. Subjects will ask to meet with the managers for a small donation of scrap copper. The group claims the donation will help disabled kids. In return for the donation they have a gift they will give the managers. Subjects have managed to take more than a small donation and later sell it for cash.

Subjects have been identified as being the same subjects that stole $40,000 pounds of copper in Seattle in April 2013, using the same MO. Subjects have also targeted power plants in Maine.

(SAR received from private sector partner on 06/07/2013)

FOR OFFICIAL USE ONLY

Infrastructure Protection Bulletin

Scrap Metal Thieves Posing as Cherokee Nation Members Seeking “Donations”

Michael George, aka “Michael Littlebear”
5’8” - 200 pounds
Brown Hair
Blue Eyes

Jim Costa, aka “Joe Wolf”
5’8” - 200 pounds
Black Hair
Brown Eyes

White Ford F350
Texas Plate #ALL0654
18’ Delta Box Trailer
Oklahoma Plate # 176-421

Details:

(FOUO) Two men posing as members of the Cherokee Nation are employing a charity ruse to steal large amounts of copper and other scrap metal from companies and utilities in Texas. The activities of Michael George, aka “Michael Littlebear,” and Jim Costa, aka “Joe Wolf,” have been reported most recently in Seattle, Washington and Lewiston, Maine, where they have previously been arrested with stolen metals and Native American trinkets used in their theft scheme. Reporting indicates that the two men, both of whom have ties to the Dallas/Fort Worth region, are now operating the scheme in Texas in search of copper and scrap metal in general.

(U) Anyone who encounters these two individuals is encouraged not to cooperate, to call police and also to report the matter to the Texas Fusion Center via www.iwatchtx.org. Law enforcement officers who encounter these individuals are encouraged to promptly investigate further for evidence of metal theft.

FOR OFFICIAL USE ONLY
Online Suspicious Activity Report

www.txdps.state.tx.us
www.iwatchTX.org
Welcome

Welcome to the DPS iWATCH website, where you can report suspicious activities or behaviors that may indicate criminal or terrorist activity.

This site is not designed to report emergencies. If this is an emergency, call 911.

Every report will be reviewed by analysts. Providing your contact information is required to ensure that DPS personnel can contact you to follow up with additional questions. If you prefer to make an anonymous report, contact DPS at 1-866-786-5872.

The report should take less than 5 minutes to complete.

Please click the button below to indicate that you agree to these terms, and to complete the report.

I Agree  Cancel
Online Suspicious Activity Report – Contact Information

iWATCH the Official Community Reporting Website of the Department of Public Safety
www.iwatchTX.org

Person Reporting

Please enter your contact information, then click "Next" to proceed.

- This contact information will be used by the Texas Department of Public Safety to follow up with you on any questions regarding your report.
- Reports with no contact information will not be accepted.

* Your Name
* Street Address (no P.O. Boxes)
* City
* State TX
* Telephone
* Zip

Email

Previous Next
Online Suspicious Activity Report – Date/Time/Involved

iWATCH the Official Community Reporting Website of the Department of Public Safety
www.iwatchTX.org

Basic Information

- When did the suspicious activity occur? 1/24/2013 at 6:40 AM
- How many people were involved? 0
- How many vehicles were involved? 0

Please provide some basic information about the incident.

- If you observed the same activity on more than one occasion, select the most recent date/time.
Enter a location and click "Go" to see the map.
Online Suspicious Activity Report – Person Information (PII)

Please describe this individual:
- Use the large blue buttons on the right to make your selections.
- To change a characteristic you have already selected, click on the label (e.g., "Gender") in the left column.
- If you have indicated that more than one person was involved, you will be asked for this information about each individual.

Gender:
Height:
Build:
Age:
Primary Hair Color:
Secondary Hair Color:
Facial Hair:
Facial Hair Color:
Complexion:
Glasses:

Do you know the person’s name or address?

Comments (clothing, distinguishing features, accessories such as bags, cameras and other notables, etc.):

Check Spelling

Previous Next
<table>
<thead>
<tr>
<th>Plate:</th>
<th>Type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country:</td>
<td>Color:</td>
</tr>
<tr>
<td>State:</td>
<td>Interior Color:</td>
</tr>
<tr>
<td>Make:</td>
<td>Age:</td>
</tr>
<tr>
<td>Model:</td>
<td>Condition:</td>
</tr>
</tbody>
</table>

Distinguishing Characteristics (Bumper stickers, damage, etc.):

Check Spelling
**Online Suspicious Activity Report - Activity**

**iWATCH the Official Community Reporting Website of the Department of Public Safety**

www.iwatchTX.org

* How suspicious was the activity?
* Was the person (or persons) attempting to conceal their behavior?
* Describe what you saw.

---

**LAW ENFORCEMENT SENSITIVE**
If you have any photo, video, or audio files of the people, vehicles, or activity, click below to upload them. Attachments are limited to 50MB.

- You can indicate which person or vehicle is shown in each attachment.
Thank You

Thank you for submitting an iWATCH report!

Every report is an important piece of the puzzle and will be reviewed by trained the Texas Department of Public Safety personnel. If there are any questions regarding your report, the Texas Department of Public Safety personnel will follow up with you using the contact information you have provided.

Return to the Texas Department of Public Safety online
Submit another iWATCH report
Contact Information

• Watch Center
  – 512-424-7981 or 1-866-786-5972
  – TXFusionCenter@dps.texas.gov

• SAR Manager
  – Lexi Quinney
    Office: 512-424-2752
    Mobile: 512-845-4958
    Lexi.Quinney@dps.texas.gov

• Critical Infrastructure Protection Program
  – Dave Jackson
    Office: 512-424-7104
    Mobile: 512-217-2983
    David.Jackson@dps.texas.gov

For Official Use Only