

When in Doubt - Report

Detection of terrorist and criminal activity is the key to preventing such acts. We have all observed activity that is “just not right”. A person that is out of place, a vehicle at a strange location or time, or an activity that should just not be happening, etc. Many times, it is after the fact we learn that what we saw in fact really was a problem. Immediate reporting of what you see could have possibly changed the outcome. **Timely reporting of suspicious incidents is the key to detecting and preventing terrorist and criminal acts.**

Both terrorist and criminals have patterns to their activities. The bits and pieces of activity that you see or hear are all indicators that help identify these patterns. Law enforcement and security professional are trained to fit these indicators together and identify the patterns so they can take proactive preventive measures. **Without the indicators, these professionals cannot identify patterns of activity.**

What should I report?

The Surface and Public Transportation ISACs are dedicated to the security of all surface and public transportation assets, systems, passengers, and commodities. The following types of events and/or suspicious activity should be reported immediately to local law enforcement and then to the ST and PT ISACs.

Suspicious Activity

Report any of the following suspicious activities. These indicators may be precursors to a terrorist attack or criminal activity but are not all-inclusive.

Surveillance

- ◆ Persons monitoring, photographing, videotaping, or making diagrams/maps of transportation vehicles, stations, platforms, bridges, tunnels, or other facilities. Report all incidents even if resolved by law enforcement and thought harmless.
- ◆ Persons in places where there is no a reasonable explanation for their presence, conducting an activity that does not fit, or carrying and/or wearing unusual items for the setting, location, or season.

Preparation

- ◆ Loss or compromise of security codes or combinations to critical facilities and IT Systems. Loss or theft of keys or access cards to critical facilities.

- ◆ Loss or theft of employee identification, access cards, or parking decals that allows access to critical facilities/functions.
- ◆ Theft of agency vehicles, radios or other communication devices.
- ◆ Loss or theft of schematic drawings, engineering plans, track diagrams, information system network diagrams or information.
- ◆ Loss or theft of transit agency uniforms, badges, patches, identification tags, etc.

Training/Rehearsals/Tests

- ◆ Multiple persons appearing to be working in unison exhibiting suspicious behavior.
- ◆ Receipt of threatening messages, telephone calls, bomb threats, etc.
- ◆ Unusual or unfamiliar vehicles parked near facilities or near large public events.
- ◆ Drivers attempting to park vehicles near large public events or inside restricted areas (such as by driving around barricades).
- ◆ Unexpected or unfamiliar delivery trucks arriving at critical facilities.
- ◆ Vehicles arriving and being left behind at unusual hours.
- ◆ Substances leaking or spilling from vehicles.
- ◆ Unexplained false burglar or fire alarms, prank calls for bomb threats, or other actions that may indicate someone testing security or emergency response.
- ◆ Persons arriving to conduct service or repairs without a valid work order or other authorization. Persons using or producing altered or fraudulent identification.
- ◆ Persons using identifications with conflicting names, addresses, social security numbers, etc.
- ◆ Incidents of unusual activity that appear to be unauthorized tampering with transit vehicles, signals, tracks, power sub stations, or other facilities.

Explosions

Any explosion on a transportation vehicle (bus, train, van, truck) or at a facility (Bus or Train Station, platform, vehicle yard, fuel centers, maintenance facilities, administrative buildings, crew areas, etc).

Suspected or confirmed Hazardous Materials Release

Any confirmed or suspected release of hazardous materials or reports of a HAZMAT release/accident should be reported. Of critical concern are reports of a Poison by Inhalation (PIH) chemical release. PIH materials are listed below:

- ◆ Chlorine

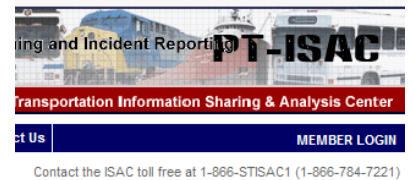
- ◆ Anhydrous Ammonia
- ◆ Ethylene Oxide
- ◆ Hydrocyanic Acid

How do I report an Incident?

(If the incident is ongoing, dial 911 and report the incident to local authorities first.)

The ST and PT-ISAC website (<http://www.surfacetransportationisac.org/>) has a link to an incident report form. Clicking on the “Submit an Incident Report” Button will open the report form.

You can also contact the ST and PT ISAC Toll Free by phone 24/7 at 1-866-STISAC1 (1-866-784-7221)



Submit an Incident Report

[Submit Incident](#)

The ST-ISAC will help ensure that intrusions on transportation information technology ... do not disrupt the nation's transportation operations.

What type of an incident is this? A cyber (computer) incident, a physical activity, or something to do with Hazardous Materials or Chemicals?

Submit an Anonymous Report

Report Type: Cyber Physical Hazmat or Contamination

Details:

Additional Comments:

Is ISAC assistance Required?
 Yes
 No

The ISAC can share this information with:
 law enforcement
 other members
 government agencies
 other ISACs

Who, What, Where, When, Why



Reports need to be concise and contain accurate information. The five “W’s” provide a good report outline.

WHO? Describe who is involved in suspicious activity.

WHAT? Describe the suspicious activity.

WHEN? Indicate if the activity is in progress or give the time(s) that the activities occurred.

WHERE? Give the location of the suspicious activity (i.e. street address or name of the facility).

WHY? Indicate why the activity is suspicious to you. If known, tell what might be the target of the activity.

Is there any additional information that you want to add? It is not required but if you would like the ST and PT-ISAC to contact you for additional information or clarification, please include your contact information. (The ST and PT ISAC **WILL NOT** release your personal information).

The reporting entity solely determines how the ISAC will handle a report. Reports can be directed to be completely anonymous. The ST and PT ISAC **WILL NOT SHARE** information with any individual or organization that you do not want the information shared.

What does the ISAC do with my Report?

First and foremost the ST and PT ISAC **DOES NOT SHARE** any information that you report that is of a sensitive nature to your organization and that you indicate on the reporting form not to share. The ST and PT ISAC combines incident report data with other classified, law enforcement, and sensitive data and performs analysis to identify any threats to the transportation industry. The ST and PT ISAC publishes a quarterly Threat Assessment to the Transportation Industry for use in Risk Management and Security System Design Efforts. The ST and PT-ISAC will share the analyzed incident data and our threat assessment with law enforcement, homeland security, and intelligence organizations.

Reporting Tips

When observing what may be deemed a suspicious activity it is important to gather as much information as possible concerning the Who, What, Where, When and How. Detailed descriptive information provided to law enforcement agencies and/or intelligence analysts is invaluable for investigation and analysis of the incident. To assist in remembering what information to gather, use the acronym CYMBALS, a popular technique for reporting details of persons or vehicles:



Color of Hair, Skin, Clothes

Year (Age) of the person

Race or ethnicity

Body - Height, weight, build

Additional Details - carrying items, backpack, camera, etc

Looks - Scars, tattoos, facial hair

Sex

C Color of the vehicle, License Plate

Y Year of vehicle

M Make of the vehicle, model

B Body - SUV, Car, Van, Truck

A Additional details - direction of travel, damage, bumper stickers

L License Number, VIN, or DOT Number

S State (License Plate)