

JOIN OPERATION SAFEGUARD

The New York State Office of Homeland Security, in conjunction with law enforcement agencies throughout New York State, is reaching out to businesses, organizations, and communities to create a better public awareness of potential terrorist indicators and suspicious activities. This outreach promotes the recognition and reporting of potential terrorist activities within the community to the New York State Terrorism Tips Hotline @ 1-866-723-3697. Additionally, businesses and community organizations will benefit from this outreach as they are provided with ways in which they can better protect themselves against loss resulting from potential terrorist and other criminal activity.



There is a concern that individuals seeking to commit acts of terrorism may utilize community organizations, as well as small businesses and corporations, to acquire certain materials, skills, or training in order to succeed with their intentions. Through visiting the Office of Homeland Security website, www.security.state.ny.us, corporations, small businesses, and community members are provided with terrorism awareness tips to help protect themselves from being a victim of potential terrorist activity. Additionally, they may choose to sign up to receive emergency alerts and advisories through www.NYALERT.gov.

Early recognition and reporting of potential terrorist activity can serve as the first line of defense against those whom intend to harm the citizens of New York State or its assets. Instances of suspicious conduct observed by members of the community may not be criminal per se, but may be peculiar and unusual because it does not match the usual pattern of daily activity found within the community. The intent is not to question or infringe upon people's daily routines and way of life, or to distrust members of the community; but rather to provide a resource to recognize and report those things that may not necessarily fall into the norm. Any signs of suspicious activity may be reported 24 hours a day, seven days a week to the New York State Terrorism Tips Hotline @ 1-866-723-3697.



Help protect your assets, while being our eyes & ears in the War on Terrorism...

If you see any of the signs of terrorism, say something

**Report any suspicious activity to the
Terrorism Tips Line at**

1-866-SAFE-NYS

1-866-723-3697

NEW YORK STATE OFFICE OF HOMELAND SECURITY

Harriman State Office Campus
1220 Washington Avenue
Building 7A
Albany, NY 12242
(518) 402-2227

NEW YORK STATE
GOVERNOR ELIOT SPITZER

OPERATION SAFEGUARD



www.security.state.ny.us

www.troopers.state.ny.us

www.nyschiefs.org

www.nysheriffs.org



Dear Participants of *Operation Safeguard*,

You have chosen to play an important role in a truly unique and notable project across New York State. I would like to thank you for your assistance and cooperation in this important endeavor. *Operation Safeguard* is an important program partnering community members, businesses, and other associations across New York State to work together to alert members of state and local law enforcement to suspicious activities and potential acts of terrorism. You are our eyes and ears on the ground- on the streets, going to grocery stores, in the mall, being an everyday citizen; you can help us to fulfill our public safety responsibilities. I ask that you continue to be vigilant, and if you see something, say something. Early recognition and reporting of potential terrorist activity can serve as the first line defense against those who commit acts of terrorism. If you witness anything suspicious, you are encouraged to contact your local law enforcement or the New York State Terrorism Tips Line at 1-866-SAFE-NYS.

Thank you for your continued vigilance.

Sincerely,

Michael Balboni
Deputy Secretary to the Governor for Public Safety
New York State

SOME WAYS THAT COMMUNITY MEMBERS CAN HELP PREVENT TERRORISM

Know the Routines. Be alert as you go about your daily business. This will help you to learn the normal routines of your neighborhood, community and workplace. Understanding these routines will help you spot anything out of place.

Be aware of what is going on around you. Whether traveling, at work or at home, be on the lookout for suspicious activities. Learn to spot suspicious mail, packages, luggage abandoned in a crowded place like an office building, an airport, a school, or a shopping center.

Take what you hear seriously. If you hear or know of someone who has bragged or talked about plans to harm citizens in violent attacks or who claims membership in a terrorist organization, take them seriously and report it to law enforcement immediately.

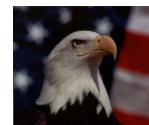


SOME WAYS THAT BUSINESSES AND ORGANIZATIONS CAN PROTECT THEMSELVES FROM LOSS

- ▶ Monitor and control who is entering your workplace: current employees, former employees, and commercial delivery and service personnel.
- ▶ Check identification and ask individuals to identify the purpose of their visit to your workplace.
- ▶ Report broken doors, windows and locks to your organization's or building's security personnel as soon as possible.
- ▶ Back-up files or copies of sensitive and critical information and databases should be made.
- ▶ Store, lock, and inventory your organization's keys, access cards, uniforms, badges, and vehicles.
- ▶ Monitor and report suspicious activity in or near your facility's entry/exit points, loading docks, parking areas, garages, and immediate vicinity.
- ▶ Suspicious-looking packages should be reported to your local police. DO NOT OPEN or TOUCH.
- ▶ Shred or destroy all documents that contain sensitive personal or organizational information that is no longer needed.
- ▶ Keep an inventory of your most critical equipment, hardware, and software.
- ▶ Store and lock your personal items such as wallets, purses, and identification when not in use.

TERRORIST GROUPS HAVE BEEN KNOWN TO...

- Establish cells and operations within the United States
- Be diverse and encompass members of different cultures
- Engage in criminal entrepreneurship for funding purposes
- Counterfeit money for funding purposes (\$100 bills and \$50 bills are the most common)
- Smuggle and traffic drugs through various means including personal vehicles, tractor trailers, motorcycles, small private planes, small boats, snowmobiles and sleds
- Engage in illegal liquor and cigarette trade
- Illegally purchase and trade weapons



KNOW THE SEVEN SIGNS OF TERRORISM

- 1) Surveillance:** Recording or monitoring activities, taking pictures, making drawings.
- 2) Elicitation:** Attempts to gain information about operations, staffing, and security.
- 3) Tests of Security:** Any attempts to measure reaction times to entering restricted areas.
- 4) Acquiring Supplies:** Obtaining explosives, weapons, uniforms, badges, credentials, etc.
- 5) Suspicious Persons Out of Place:** This may include people who are in places they should not be, as well as people who do not fit in to the daily routine of your neighborhood or community.
- 6) Dry or Trial Run:** Putting people into position and moving them around without actually committing a terrorist act.
- 7) Deploying Assets:** People and supplies getting into position to commit the act.

RECOGNIZE SUSPICIOUS CYBER INCIDENTS

- ▶ **System Failure or Disruption:** Disruptions in the availability of your system or website; employees, customers, suppliers, members, or partners unable to access your system or website; or service being denied to its users.
- ▶ **Suspicious Questioning:** Attempts to gain information in person, by phone, mail, e-mail, etc., regarding the configuration and/or cyber security posture of your website, network, software, or hardware.
- ▶ **Unauthorized Access:** Anyone attempting (failed or successful) to gain unauthorized access to your system or its data.
- ▶ **Unauthorized Changes or Additions:** Unauthorized changes or additions to your system's hardware, firmware, or software characteristics without your IT department's knowledge, instruction, or consent.
- ▶ **Suspicious E-mails:** Anyone in your organization has received suspicious e-mails that include unsolicited attachments and/or requests for sensitive personal or organizational information.
- ▶ **Unauthorized Use:** Unauthorized parties using your system for the processing or storage of data or former employees, customers, suppliers, or partners still using your system.