



Hundreds of thousands of religious facilities serve millions of people of all faiths and denominations throughout the United States. Religious facilities are generally open-access public assembly venues and have been successfully targeted by terrorists on numerous occasions in the past.



Potential Indicators of Terrorist Activity

Terrorists have a wide variety of weapons and tactics available to achieve their objectives. Specific threats of most concern to religious facilities include:

- ☒ Improvised explosive devices (IEDs)
- ☒ Arson/ incendiary attack
- ☒ Small arms attack
- ☒ Assassination/kidnapping
- ☒ Chemical/biological/radiological agent attack

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack. Indicators of an imminent attack requiring immediate action may include the following:

- ☒ Persons in crowded areas (e.g., reception or meeting areas) wearing unusually bulky clothing that might conceal suicide explosives or weapons
- ☒ Suspicious or illegally parked vehicles near facility or near places where crowds gather
- ☒ Unattended packages (e.g., backpacks, briefcases, boxes) that might contain explosives
- ☒ Suspicious package or letter received by mail that might contain explosives or chemical, biological, or radiological agent

- ☒ Unexpected or unfamiliar delivery or maintenance vehicles
- ☒ Evidence of unauthorized access to areas of the building containing heating, ventilation, and air-conditioning (HVAC) equipment

Indicators of potential surveillance by terrorists include:

- ☒ Persons using or carrying video/camera/observation equipment in or near the facility over an extended period
- ☒ Persons discovered with facility maps, photos, or diagrams with critical assets highlighted or listing of personnel
- ☒ Persons questioning religious facility employees off-site about practices pertaining to the facility and its operations
- ☒ Persons parking, standing, or loitering in the same area over a multiple-day period with no reasonable explanation
- ☒ Facility employees associating with suspicious individuals
- ☒ An increase in threats from unidentified sources by telephone, postal mail, or e-mail and/or an increase in reports of threats from outside known, reliable sources

Common Vulnerabilities

The following are key common vulnerabilities of religious facilities:

- ☒ Significant numbers of people of like faith gathered in a single symbolic location at specified times
- ☒ Generally unrestricted access to religious services
- ☒ Unrestricted access to peripheral areas, such as contiguous parking areas and separate educational facilities
- ☒ Building systems that are vulnerable to fire, contamination via heating and cooling systems, explosives, and blocked emergency exits
- ☒ Access by workers and maintenance staff who may not undergo background checks
- ☒ Easy facility identification either by facility configuration, design, or signage
- ☒ Non-profit status, which may result in limited resources for security

Protective Measures

Protective measures include equipment, personnel, and procedures designed to protect a facility against threats and to mitigate the effects of an attack. Protective measures for religious facilities include:

☒ Planning and Preparedness

- ☒ Designate an employee as security director
- ☒ Develop a comprehensive security plan and emergency response plan for the facility
- ☒ Establish liaison and regular communication with local law enforcement and emergency responders
- ☒ Conduct regular exercises with facility employees to test the security and emergency response plans

☒ Personnel

- ☒ Conduct background checks on all employees
- ☒ Incorporate security awareness into employee training programs
- ☒ Maintain an adequate security force using both employees and congregation volunteers

☒ Access Control

- ☒ Define the facility perimeter and areas within the facility that require access control
- ☒ Limit access to congregation members and visitors to a level consistent with facility operations
- ☒ Keep vehicles away from critical assets and from areas where large numbers of people congregate
- ☒ Require that all illegally parked vehicles be moved or have them towed
- ☒ Provide adequate door and window locks, barred entryways, and fencing and gate locks to areas where access is to be limited; add intrusion detection systems and alarms as appropriate
- ☒ Train mail room and receiving personnel to recognize suspicious mail, packages, shipments, or deliveries

☒ Barriers

- ☒ Evaluate the need for perimeter barriers (e.g., fences, berms, concrete walls) around the facility
- ☒ Establish a clear zone adjacent to sensitive or critical buildings; keep zone free of vegetation and other obstructions to allow for continuous monitoring
- ☒ Install barriers to protect doors and windows from small arms fire and explosive blast effects
- ☒ Install barriers at HVAC systems to prevent the introduction of chemical, biological, or radiological agents into the building

☒ Communication and Notification

- ☒ Install system(s) that provide communication with all individuals at the facility, including employees, security force personnel, congregation members, and visitors
- ☒ Develop a notification protocol that specifies who should be contacted in emergencies

☒ Monitoring, Surveillance, Inspection

- ☒ Evaluate needs and design a monitoring, surveillance, and inspection program that is consistent with facility operations and security requirements
- ☒ Provide visual surveillance capability for sensitive and critical assets at the facility
- ☒ Continuously monitor all people entering and leaving the facility; train monitors to detect suspicious behavior

☒ Infrastructure Interdependencies

- ☒ Ensure that the facility has adequate utility service capacity to meet normal and emergency needs
- ☒ Secure dumpsters and other trash containers to prevent the hiding of explosives or other hazardous materials

☒ Cyber Security

- ☒ Develop and implement a security plan for computer and information systems hardware and software
- ☒ Design and implement a secure computer network architecture
- ☒ Regularly review facility Web site to ensure that no sensitive information is provided

☒ Incident Response

- ☒ Ensure that an adequate number of emergency response personnel are available at all times
- ☒ Check the status of all emergency response equipment and supplies on a regular basis
- ☒ Identify entry and exit points to be used in emergencies
- ☒ Ensure that employees are familiar with procedures for shutting off utility services (e.g., electricity, natural gas) in emergency situations

WARNING

This document is **FOR OFFICIAL USE ONLY (FOUO)**. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

At a minimum when unattended, this document is to be stored in a locked container such as a file cabinet, desk drawer, overhead compartment, credenza or locked area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

*For more information about this document contact:
Protective Security Coordination Division
(IPassessments@dhs.gov or FOBanalysts@dhs.gov)*

7. Deploying Assets

Look for someone deploying assets or getting into position. This is your last chance to alert authorities before a terrorist act occurs. It is also important to remember that pre-incident indicators may be months or even years apart. Therefore, it is extremely important to document every fragment of information, no matter how insignificant it may appear. This information should be forwarded immediately to NJOHSP at the 24-hour toll-free hotline 1-866-4SAFENJ, 2-1-1, or by emailing tips@njohsp.gov.

8. Terrorism Funding

Terrorists use a variety of methods to raise, launder, and transport funds. Possible indicators include, but are not limited to:

- Suspicious credit card applications
- Suspicious spending
- Multiple surnames at the same address
- Illegal drugs
- Bulk purchases of cigarettes or other counterfeit goods



The Five W's: What To Remember When Reporting Suspicious Activity

What is happening?

Who is doing it?

Where is it taking place?

When did you observe it?

Why are you suspicious?

Learn More About
Terrorism Indicators:

www.NJHomelandSecurity.gov
[Facebook.com/NJOHSP](https://www.facebook.com/NJOHSP)
[Twitter.com/NJOHSP](https://twitter.com/NJOHSP)
[@NJOHSP](https://www.instagram.com/NJOHSP) | [#NJOHSP](https://www.tiktok.com/@NJOHSP)

NJOHSP



8 Signs of Terrorism

Report Suspicious Activity
tips@njohsp.gov
866.4.SAFENJ or 2.1.1

www.NJHomelandSecurity.gov



1. Surveillance

The first sign of terrorism is someone trying to monitor or record activities. If terrorists are targeting a specific area, they will most likely be observed in that location during the planning phase. Terrorists will attempt to determine the strengths, weaknesses, and number of personnel that may respond to an incident. Routes to and from the target are usually established during the surveillance phase. It is important to note the following suspicious actions:

- Using cameras (still or video)
- Drawing diagrams or annotating maps
- Using vision-enhancing devices
- Possessing floor plans or blueprints of places such as high-tech firms, financial institutions, or government and military facilities.

Any of these acts may be an indicator that something is not right, and they should be reported immediately.

2. Elicitation/Seeking Information

The second sign is an attempt to gain information through inquiries, including seeking knowledge about a place, person, or operation. Elicitation can be made by telephone, mail, fax, or in person. Examples include inquiries about critical infrastructure such as a power plant, water reservoir, or maritime port. Terrorists may attempt to research bridge and tunnel use, make unusual inquiries concerning shipments, or look into how a facility operates. They may also attempt to place “key” people in sensitive work locations to gain intelligence.

3. Tests of Security

Tests of security or probing are techniques terrorists use to gather data. These are usually conducted by driving past or even penetrating the target, moving into sensitive areas, and observing security and law enforcement responses. Terrorists may also try to penetrate physical security barriers or test response procedures to assess strengths and weaknesses. Specific areas of interest might include the number of response personnel and routes taken to a specific location. Vehicles parked for unusually long periods of time, sometimes in no-parking zones, are another test of security.

4. Acquiring Supplies

The fourth sign of terrorism includes the purchase or theft of explosives, weapons, or ammunition. It could also include unusual purchasing or storing of fertilizer or harmful chemicals. Terrorists also find it useful to acquire law enforcement equipment and identification, military uniforms and decals, and flight passes, badges, or manuals. Terrorists often use false or stolen identification documents, including passports and driver’s licenses. They may try to produce counterfeit identification by photocopying. Any of these items would facilitate entry to secure or prohibited areas. Anyone wearing a uniform or working at a sensitive facility should protect their identification documents.

***“If You See Something,
Say Something.”***

5. Suspicious People

Another pre-incident indicator is observing suspicious people who do not belong. The suspicious person could be anyone in a building, neighborhood, or business establishment who seems out of place because of their demeanor or who asks unusual questions. Suspicious persons could also include stowaways aboard ships or people jumping ship in ports.

- ***We do not profile individuals. We profile behaviors.***

6. Dry Run

A dry run may be the heart of an attack’s planning stage. Before the execution of an operation, a practice trial is usually run to work out any flaws or unanticipated problems. This is especially true for kidnappings and bombings. If you see someone monitoring a police radio frequency and recording response times, you may be observing a dry run.



GOVERNMENT OUTREACH ALLIANCE

New Jersey Office of Homeland Security and Preparedness

Director of Communications Stephanie Raphael | 609.584.4392 | sraphael@njohsp.gov
Intelligence Division John Paige | 609.815.5072 | jpaige@njohsp.gov
Deputy Director of Communications Patrick Meagher | 609.584.4823 | pmeagher@njohsp.gov
www.njohsp.gov | @NJOHSP | communications@njohsp.gov

New Jersey State Police

Captain Stephen Jones | 609.882.2000 ext. 6513 | lpp5363@gw.njsp.org
Lieutenant Brian Polite | 609.882.2000 ext. 6514 | lpp5881@gw.njsp.org
Sergeant First Class Greg Williams | 609.882.2000 ext. 6515 | lpp4756@gw.njsp.org
www.njsp.org | @NJSP | webmaster@gw.njsp.org

New Jersey Office of the Attorney General

Assistant Attorney General Wanda Moore | 609.984.3425 | Wanda.Moore@lps.state.nj.us
Special Assistant to the Attorney General, David Frankel | 609.984.9579 |
David.Frankel@lps.state.nj.us
www.nj.gov/oag

US Attorney's Office

Community Outreach Coordinator Mikie Sherrill (USAO) | 973.645.2732 |
mikie.sherrill@usdoj.gov
Conciliation Specialist Linda Ortiz (USDOJ) | 212.264.0703 | linda.ortiz@usdoj.gov
www.usdoj.gov/crs | www.justice.gov/crs

Federal Bureau of Investigation

Community Outreach Coordinator Kimberly McDonald | 973.792.3066 |
kimberly.mcdonald@ic.fbi.gov
Special Agent Vernon Addison | 973.792.3000 | vernon.addison@ic.fbi.gov
www.fbi.gov | @FBI

US Department of Homeland Security

PSA Brian Lacey | 973.494.4225 | brian.lacey@hq.dhs.gov
Center Deputy Director Jannah Scott | Jannah.Scott@fema.dhs.gov
www.dhs.gov | @DHSgov

