

The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

2016 ADEM Surface Water Meeting

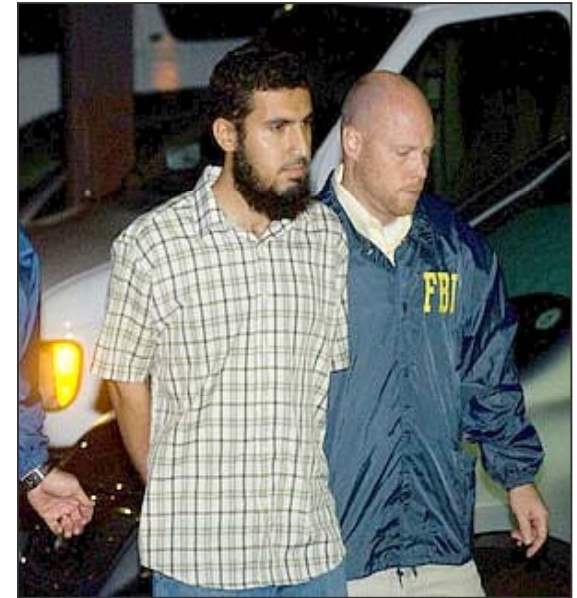
October 27, 2016



Homeland
Security

Trends and Tactics

- Tactics, techniques, and procedures evolve quickly and adapt to countermeasures
 - Explosives and improvised explosive devices (IEDs) can be manufactured out of common household products
 - Despite countermeasures to make explosives and IEDs difficult to conceal, adversaries remain adaptive
- Plots disrupted in NY, NC, AR, AK, TX, and IL during the past year were unrelated operationally, but indicative of a common cause that rallies independent extremists to want to attack the United States
- Pre-operational indicators are becoming more and more difficult to detect, therefore State, local, and private sector partners play a critical role in identifying and reporting suspicious activity



Najibullah Zazi (Denver Post)



September 25, 2009 Zazi purchasing chemicals (CNN)



**Homeland
Security**

Small Unit Assaults

- Terrorists continue to use small-unit assault tactics overseas
- Small-unit attacks typically feature more advanced levels of planning, training, and preparation and may involve one or more mobile assault teams attacking a single target or several small mobile teams attacking multiple targets for extended periods
- On June 28 and 29, 2011, nine terrorists—several wearing suicide vests and carrying small arms, rocket-propelled grenades, and hand grenades—infilitrated and conducted a night attack against the Intercontinental Hotel in Kabul, Afghanistan (12 people and all nine attackers killed, 20 people wounded)
- Several small teams totaling 10 operatives used small arms, grenades, and explosives in attacks against hotels, a train station, and other public facilities in Mumbai, India on November 26-28, 2008 (166 people and 9 of 10 attackers killed)



Potential Indicators

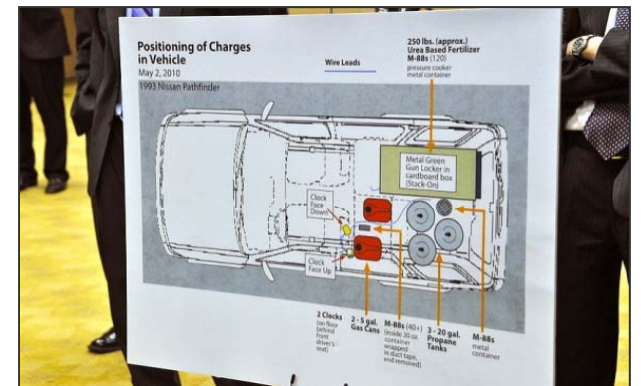
- Employees being questioned offsite about practices pertaining to the potential target
- A noted pattern or series of false alarms requiring a response by law enforcement or emergency services
- Unusual or unannounced maintenance activities in the vicinity of the store
- Persons using or carrying video/camera/observation equipment over an extended period
- Unattended vehicles illegally parked near the buildings or places where large numbers of patrons gather

Disrupted Plots: 2010 Times Square

- Faisal Shahzad was sentenced to life in prison for attempting to set off a bomb in Times Square in New York City on May 1, 2010
 - Car spotted by two street vendors who noticed smoke emanating from vents near the back seat of the unoccupied vehicle, which was parked with its engine running and its hazard lights on
 - The street vendor alerted a mounted policeman
 - The bomb had been ignited, but failed to explode, and was disarmed before it caused many casualties
- Based on initial observations, this indicates:
 - Overseas bomb-making training
 - Compressed planning cycle
 - Legal purchase of precursor materials
 - Continued terrorist interest in soft targets



May 2010 Times Square VBIED Attempt (Reuters)



Justice Department diagram of VBIED



**Homeland
Security**

Disrupted Plots: 2007 London

- An ambulance crew — responding to a call just before 1:30 a.m. about a person who had fallen at a Haymarket nightclub — noticed smoke coming from a car parked in front of the building
- The first car was a metallic green Mercedes packed with petrol, gas canisters, and nails
- The second car, a blue Mercedes, was parked a few hundred yards from the first, but was towed after being issued a parking ticket at around 2:30 a.m.
 - Staff at the car pound alerted police because “it smelled of gas”



Mercedes found in central London (FOX News)



Disrupted Plots: 2007 Fort Dix

- Six men were convicted of plotting to attack Fort Dix, a U.S. Army post in New Jersey
 - A Circuit City employee alerted local police about a video that depicted disturbing images of men firing rifles and calling for jihad. The employee had been asked by members of the group to convert the 8mm videotape to a DVD
 - The arrests were made after a 16-month FBI operation that included infiltrating the group



Fort Dix Entrance (NY Times)



**Homeland
Security**

Disrupted Plots: 2006 Toledo

- Three men were convicted of plotting to recruit and train Iraqi insurgents and kill U.S. troops overseas
 - The men, including a University of Toledo computer and engineering student, planned to wage “holy war” using skills learned via the Internet, and they intended to enter Iraq under the guise of doing business related to a used-car lot that one of them owned
- A man that had been approached by one of the men to provide security and bodyguard training to the group came forward to the authorities
- Other members of the Muslim community also went to Federal authorities with information regarding “violent and radical” statements made by the men

Disrupted Plots: 2004 London

- Five men were sentenced to life in prison for plotting to blow up a shopping center in Kent and a nightclub in London with massive fertilizer bombs
- An agricultural merchant was bemused by the request of a flashy young man that arrived in a customized Audi, rap music blaring, that asked for a half ton of ammonium nitrate fertilizer
 - The salesman noted that it was winter and the order was enough to cover five soccer fields
 - The salesman questioned the customer's intentions and sarcastically asked if he was planning a bombing attack
- Staff at Access Storage near Heathrow contacted police after the tenant refused to answer questions about why he was paying £207 a month to store £90 worth of fertilizer



Storage depot where fertilizer was discovered (LIFE magazine)



General Protective Measures

- Planning and Preparedness
 - Develop comprehensive security and emergency response plans
 - Develop policies and procedures for dealing with hoaxes and false alarms
 - Test plans prior to an emergency to ensure preparedness
 - Post Department of Homeland Security (DHS) Bomb-making Materials Awareness Program register cards and break room posters
 - Review DHS Active Shooter training materials
- Personnel
 - Incorporate awareness and response procedures into employee training programs
 - Attend DHS Private Sector Counterterrorism Awareness Workshop
- Access Control
 - Remove any vehicles that have been parked for an unusual length of time
- Barriers
 - Install and inspect blast-resistant trash containers
 - Install active vehicle crash barriers to protect buildings and populated areas



General Protective Measures (cont.)

- **Monitoring, Surveillance, Inspection**
 - Regularly inspect lockers, trash bins, parking lots, and secure areas
 - Evaluate needs and design a monitoring, surveillance, and inspection program consistent with store operations and security requirements
- **Communications**
 - Take any threatening or malicious telephone calls, facsimile, or bomb threat seriously
 - Develop a communication and notification plan
 - Consider having prerecorded announcements to play for emergencies
- **Infrastructure Interdependencies**
 - Provide for redundancy and emergency backup capability for supply systems
 - Locate the redundant and backup equipment in a different part of the store than used for the primary supply equipment, so primary and backup equipment will not be affected by a single incident



Al-Qaeda Casing Report

- Building construction vulnerabilities: Abundance of glass and its destructive power is noted throughout each of the casing reports
- Other building vulnerabilities noted:
 - Building set back
 - Location of HVAC systems
 - Substandard weight-bearing columns
 - Lack of emergency exits and escape routes
 - Inadequate sprinklers and fire detection systems
 - Focus on the physical construction of the buildings

Protective Security Advisors

- 96 PSAs and Regional Directors, including 89 field deployed personnel, serve as critical infrastructure security specialists
- Deployed to 73 Districts in 50 states and Puerto Rico
- State, local, tribal, and territorial link to DHS infrastructure protection resources
 - Coordinate vulnerability assessments, DHS products and services, and training
 - Provide vital link for information sharing
 - Assist facility owners and operators with obtaining security clearances

Enhanced Critical Infrastructure Protection

- ECIP Initiative
 - Identifies facilities' physical security, security forces, security management, protective measures, information sharing, and dependencies
 - Provides comparison across like assets and tracks implementation of new measures
 - Informs facility owners and operators of the importance of their facilities as an identified high-priority infrastructure and the need to be vigilant
 - Establishes/enhances relationships with facility owners and operators
- Infrastructure Survey Tool (IST)
 - Over 1,400 IST surveys conducted to date
 - Apply weighted scores to identify vulnerabilities and trends for infrastructure and sectors and conduct sector-by-sector and cross-sector vulnerability comparisons
 - Facilitate the consistent collection of facility security information
 - Provide information for protective measures planning and resource allocation
 - Enhance overall capabilities, methodologies, and resource materials for identifying and mitigating vulnerabilities

Homeland Security Information Network

- HSIN is DHS's primary technology tool for trusted information sharing
- HSIN – Critical Sectors (HSIN-CS) enables direct communication between DHS, Federal, State, and local governments, and infrastructure owners and operators
- Content Includes:
 - Planning and Preparedness: Risk assessments, analysis, guidance, and security products; geospatial products and hurricane models; exercise and national event info
 - Incident Reporting and Updates: Real-time situational reports and alerts
 - Situational Awareness: Numerous recurring daily and monthly sector-specific and cross-sector reports on topics ranging from cybersecurity to emerging threats
 - Education and Training: Training on topics ranging from critical infrastructure resilience to threat detection and reaction for retail staff



**Homeland
Security**

TRIPwire and TRIPwire Community Gateway

- TRIPwire – Online unclassified network for law enforcement having bombing prevention responsibilities to discover and share tactics, techniques, and procedures of terrorist IED use
 - Combines expert analysis with relevant documents gathered from terrorist sources to assist law enforcement’s ability to anticipate, identify, and prevent IED incidents
- TRIPwire Community Gateway – Brings timely bombing prevention awareness information and analysis to the private sector with bombing prevention responsibilities
 - Responds to increasing private sector demand for bombing prevention information and assistance
 - Leverages content, expertise, and reputation of the existing TRIPwire system
 - Shares information on common site vulnerabilities, potential threat indicators, and effective protective measures for the 18 critical infrastructure sectors through HSIN-CS



Risk Mitigation Training

- IED Awareness/Bomb Threat Management Workshop
 - Provides an IED overview and focuses on the steps for managing bomb-related threats by outlining specific mitigation and response strategies to deal with explosive incidents and bomb threats
- IED Search Procedures Workshop
 - Enhances participants' knowledge of IED awareness, prevention measures, and planning protocols by outlining specific search techniques that reduce vulnerability and mitigate the risk of terrorist IED attacks
- Protective Measures Course
 - Provides owners and operators in the public/private sector with the knowledge to identify the appropriate protective measures for their unique sector
- Surveillance Detection Course for Law Enforcement & Security Professionals
 - Provides participants with the knowledge, skills, and abilities to detect hostile surveillance conducted against critical infrastructure
- IED Counterterrorism Workshop
 - Enhances the knowledge of State and local law enforcement and public/private sector stakeholders by providing exposure to key elements of the IED threat, surveillance detection methods, and soft target awareness
- Counter-IED/Bomb Threat Management Workshop (Executive Level)
 - High-level workshop, designed for executives and critical infrastructure owners, provides exposure to key elements of the IED threat, soft target awareness, bomb threat management planning, and mitigation cost considerations in order to inform risk management planning



National Terrorism Advisory System

- The National Terrorism Advisory System (NTAS) replaces the former DHS color-coded Homeland Security Advisory System
- Regarding a potential threat, after reviewing the available information (intelligence), the Secretary of Homeland Security will decide, in coordination with other Federal entities, whether an NTAS Alert should be issued
- NTAS Alerts will only be issued when credible information is available

National Terrorism Advisory System - Alerts

- Alert Announcements
- NTAS alerts will be issued through State, local, tribal, and territorial partners; the news media; and directly to the public via the following channels:
 - Via the official DHS NTAS webpage – <http://www.dhs.gov/alerts>
 - Via email signup at – <http://www.dhs.gov/alerts>
 - Via data feeds, web widgets, and graphics – <http://www.dhs.gov/alerts>
 - Via social media
 - Facebook – <http://facebook.com/NTASAlerts>
 - Twitter – <http://www.twitter.com/NTASAlerts>
- The public can also expect to see alerts in places, both public and private, such as transit hubs, airports, and government buildings

The Nationwide Suspicious Activity Reporting Initiative

- In March 2010, the NSI Program Management Office was established within the U.S. Department of Justice (DOJ), Bureau of Justice Assistance, and is an interagency office composed of representatives from DOJ, DHS, Federal Bureau of Investigation (FBI), and the Program Manager – Information Sharing Environment office
- The NSI establishes standards, policies, and processes for gathering, documenting, processing, analyzing, and sharing SAR while taking into account the protection of privacy, civil rights, and civil liberties of Americans
- The NSI program includes training for line officers, analysts, and chief executives, as well as community outreach and a comprehensive privacy framework
- The FBI eGuardian Program is an integral part of the NSI, ensuring that information is getting from the field to the FBI Joint Terrorism Task Force for investigation
- The NSI closely coordinates with the DHS Office of Intelligence and Analysis (I&A) which leads interagency support to the National Network of Fusion Centers



**Homeland
Security**



BJA
Bureau of Justice Assistance
U.S. Department of Justice



“If You See Something, Say Something™”


- In July 2010, DHS, at Secretary Janet Napolitano's direction, launched a national "If You See Something, Say Something™" public awareness campaign
- The campaign was originally used by New York's Metropolitan Transportation Authority, which licensed the use of the slogan to DHS for anti-terrorism and anti-terrorism crime related efforts
- The campaign is a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper State and local law enforcement authorities
- Underscores the critical role that the public plays in keeping our nation safe
- DHS is launching the campaign in conjunction with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)



**Homeland
Security**

“If You See Something, Say Something™”


- Only reports that document **behavior reasonably indicative of criminal activity related to terrorism** will be shared with Federal, State, local, tribal and territorial partners
- Factors such as race, ethnicity, national origin, or religious affiliation alone are not suspicious. For that reason, the public should report only suspicious behavior and situations (e.g., an unattended backpack in a public place or someone trying to break into a restricted area) rather than beliefs, thoughts, ideas, expressions, associations, or speech unrelated to terrorism or other criminal activity



if you
SEE
something
SAY
something™

Report suspicious activity.
Contact local
law enforcement.

Did you **SEE** something suspicious?
Then **SAY** something to local law enforcement to make it right.

 **Homeland Security**

If You See Something Say Something™ used with permission of the NY Metropolitan Transportation Authority.