



Washington Regional Threat and Analysis Center

Washington, D.C.
wrtac@dc.gov
202-481-3007
202-563-2768 (Fax)



Washington DC Threat Level



Alert Level Yellow
ELEVATED CONDITION



Officer Safety & Criminal Intelligence Issues

VOLUME: 3, ISSUE: 21

EFFECTIVE DATE: 30 November 2009

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement officers, security personnel, antiterrorism officers and intelligence personnel. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and security of installation personnel, equipment and facilities. This document shall not be furnished to the media or any other agencies outside of law enforcement. It contains information that may be exempt from public release under the Freedom of Information Act (5 USC 552).

OFFICER SAFETY AWARENESS

SPRING ASSISTED TITANIUM SCREWDRIVER: This Officer Safety Item is a spring-assisted titanium screwdriver. While it appears to be a pen when carried in a pocket, it has a button that releases and locks the shaft in place. When engaged, this item could quickly become a dangerous stabbing weapon. The overall length is 6-inches with a 3.312-inch shaft. Law Enforcement and Security Professionals should be mindful of concealed weapons such as these. We are entering the season where bulky clothing will likely be worn by suspects. Always maintain positive control of a suspect's hands during a search or security inspection. Airport and transportation security screeners should also be mindful of items that appear to be pens or other common items.



Source: NYPD / Peel Regional Police – Daily Open Source Briefing Notes, 17 November 2009

CLUB / KNIFE: On Wednesday, November 4, 2009, a police officer in the 62 Precinct, recovered the below “police type” club knife from a perpetrator within the confines of the 62 Precinct. Officers should be aware that covert knives are commonly utilized on the street and are readily available via numerous sources, including the internet.



Source: MTA – NY Police Department, Daily Intelligence Briefing, 18 November 2009 / NYPD – Transit Bureau, Transit District 23

WHAT OFFICERS NEED TO KNOW ABOUT SUICIDE BOMBERS: Speaking at the IACP annual conference, Walter Purdy (former marine and current Vice President of the Terrorism Research Center) clicked through slides of photos he had taken while visiting the sites of some of the most horrific terrorist attacks in the Middle East. After providing a history of suicide terrorism dating back to ancient times, Purdy described various methods of recruitment and some of the technology employed in suicide bomb attacks. He also revealed the most potent prevention method against suicide bombers: catching the intelligence gatherers.

The bomb carriers often are carefully recruited by coercion, psychological manipulation, and appeals to disillusioned or disenfranchised young people. Those recruited or coerced into attacks are determined to die. They expect no escape and the reward of a rich afterlife.

Once an attack is underway there is no strategy for repelling the terrorists other than killing them. A consistent characteristic of these attacks is the intelligence gathering effort that precedes them. Each case study described by Purdy was a case of exploited vulnerabilities discovered by patient gathering of information by operatives.

While intrigue, sophistication, and technology may be used to plan many aspects of a suicide attack, planners rely significantly on eye witness intelligence gathering to formulate their plans. Police agencies have spent time training for responses to suicide bombers, school shooters, and active threats but there has been little emphasis on watching for precursors to these attacks; recruitment of bombers and surveillance of targets. Purdy described in detail case after case of how operatives had watched locations for days gathering intelligence such as delivery times, staffing levels, traffic patterns, and other routines to discover vulnerabilities. In successful attacks, no one had challenged suspicious behavior of persons standing hour after hour watching potential targets.

In one case a female operative had been approached by three separate police officers over a course of days asking her out while she was conducting surveillance on a restaurant later hit by a suicide bomber. The operative noticed that a security officer failed to search a musician's guitar case upon entering the restaurant. Soon after, a bomber carried out an attack using an explosive in a guitar case he brought into the restaurant.

Noting the recent case in Colorado where a suspect was found to have made several trips to a beauty supply wholesale store purchasing unusual quantities of chemical used for bomb making, Purdy related that he was able to purchase multiple batteries, wire, and other bomb material at a New York City hardware store without raising suspicion, even though he was deliberately obvious about it. The message was clear: patrol officers and citizens reporting suspicious behavior are key to preventing the inevitable proliferation of suicide attacks on American soil.

Years ago a veteran officer heard me complaining about having to respond to a barking dog call. He explained that sometimes a barking dog means a prowler or burglar is near. I remembered his words a few years later after barks led me to a car break-in where I was able to arrest the perpetrator at the scene. Purdy is reminding us that terrorism can be defeated with some good old fashioned police skills that include checking out suspicious person complaints and keeping in touch with our citizens. The suspicious person call may be the barking dog that alerts us to a planned suicide bombing.

Joel Shults currently serves as Chief of Police for Adams State College in Alamosa, Co. Over his 30 year career in uniformed law enforcement and in criminal justice education Joel has served in a variety of roles: academy instructor, police chaplain, deputy coroner, investigator, community relations officer, college professor, and police chief, among others. Shults earned his doctorate in Educational Leadership and Policy Analysis from the University of Missouri, with a graduate degree in Public Services Administration and bachelors in Criminal Justice Administration from the University of Central Missouri. In addition to service with the US Army military police and CID, Shults has done observational studies with over fifty police agencies across the country. He currently serves on a number of advisory and advocacy boards including the Colorado POST curriculum committee as a subject matter expert.

Source: IACP Digest

SEARCH OF A VEHICLE'S ELECTRONIC MEMORY: Due to the increased sophistication of automobile electronics, criminal investigators should consider establishing probable cause for a search of the automobile's electronic memory prior to the execution of a search warrant on a suspect's vehicle. Newer vehicles are commonly installed with Bluetooth technology which allows cellular telephones to link with the automobile and allow for hands free operation of the phone. Bluetooth technology can download or synchronize the cellular handset's contact list to the vehicle's electronic memory storage. The contact list/phonebook capacity varies from just over 100 to upwards of 10,000 entries according to the particular system installed. These entries can be stored and accessible even after the phone is no longer linked to the vehicle and after the ignition is disengaged. If a navigation system is also installed in the vehicle, the contact list may have addresses or GPS coordinates associated with the phone number entries. Although Bluetooth technology allows for two-way exchange of data, the Bluetooth Profile implemented in vehicle systems does not allow phonebooks downloaded from one cellular handset to be uploaded to another handset or device. Thus, agents executing a search warrant should be prepared to manually record searched entries. The current trend indicates Bluetooth technology will become more common in vehicles as a means of operating a cellular phone while driving. California, Connecticut, New Jersey, New York, Oregon, Washington State, the District of Columbia, and the U.S. Virgin Islands have all adopted laws

banning drivers from talking on handheld cellular phones while driving, with momentum building for the passage of laws in other states. Whereas a few years ago, only high end vehicles from luxury manufacturers provided Bluetooth technology as an option, many manufacturers offer Bluetooth technology as a factory installed option on lower end models such as the Ford Focus. MSNBC reports that by 2013, approximately 30 percent of all new car sales will be purchased with hands-free features onboard. Numerous suppliers and manufacturers offer aftermarket kits to install the technology in vehicles lacking factory installation and the kits are selling in the millions. The exploitation of this feature presents investigators with a possible wealth of investigative evidence to be obtained from target's vehicle by utilizing a search warrant to access the vehicle's electronic memory. The search of a vehicle's electronic systems for navigation information or telephone, address, or calendar information stored in a vehicle via a Bluetooth connection implicates the 4th Amendment. A search warrant or an exception to the search warrant requirement, such as exigent circumstances, search incident to arrest, or the vehicle exception may be required to conduct the search.

Comment: This document is the property of the Drug Enforcement Administration (DEA) and is marked Law Enforcement Sensitive (LES). Further dissemination of this document is strictly forbidden, except to other law enforcement agencies for criminal law enforcement purposes. The following information must be handled and protected accordingly. Precautions should be taken to ensure against unauthorized access and that this information is stored and/or destroyed accordingly.

Source: DEA - Office of Investigative Technology

SECURE PURSE: This officer safety/awareness item is being shared to remind all to never take anything for granted. With today's technology, items that appear to be constructed for the normal use are often made for multiple purposes. This woman's purse comes with a locking zippered gun compartment with an internal holster. It is being advertised as being extremely nice, stylish, medium-sized 10" X 9" leather handbag with two large zipper openings in the top, smaller zipper compartments on both the front and back of the purse, as well as two cell phone and/or accessory pockets on one end in addition to the weapon concealment compartment on the opposite end. The links provided below has items similar to the pictured item:



<http://www.gungear.com/index.html>

<http://mygunpurses.com/7086.aspx>

<http://www.buygunholsters.com/cogunpu.html>

Source: NY MTA Daily Intelligence Summary November 19, 2009

GANG INITIALS AND GANG NAMES

AB - Aryan Brotherhood: A white supremacist prison gang founded in the California prison system in the 1960s. The shamrock and 666 tattoos are associated with this gang.

ABT - Aryan Brotherhood of Texas: A white supremacist prison gang founded in Texas.

ABZ - Asian Boyz: An Asian-American street gang that originated in Southern California. They have spread to many parts of the U.S. and are reportedly one of the largest Asian street gangs in the U.S.. Tiny Rascal Gangsters (TRG) is one of the key rivals of this gang.

AC - Aryan Circle: A white supremacist prison gang that has spread to many other states.

AKB - Asian Killa Boyz: A Southern California street gang.

ALK - Almighty Latin Kings: Founded in Chicago, Illinois, they are one of the largest Hispanic gangs in the United States. They're also known as the Latin Kings (LK), Almighty Latin King Nation (ALKN), and Almighty Latin King and Queen Nation (ALKQN).

BA - Barrio Azteca: Founded in the 1980s, Barrio Azteca is a Hispanic prison gang active in the Southwestern United States.

BB – Border Brothers: The "Border Brothers", a Hispanic gang, are mainly found in the California Prison system, but are slowly spreading to other systems.

BD - Black Disciples: An African-American street gang founded in Chicago.

BDS - Fresno Bulldogs: A predominantly Hispanic street gang in Fresno, California. Also known as the F-14 Bulldogs.

B.E.S.T. – Barrio Eighteenth ST (Street): A violent Hispanic gang that accepts members from all ethnicities. It has spread throughout the U.S.

BGF - Black Guerrilla Family: An African-American, anti-establishment, prison gang; formed in 1966, at San Quentin State Prison in California.

BHS – Ben Hill Squad: An Atlanta, GA area street gang

BP - Brown Pride: A Mexican-American street gang found in multiple locations, including California and Arizona. BP13 and BPX3 are a couple of other tags associated with this gang.

BPS - Black P. Stones: An African-American gang founded in Chicago in the mid-20th century. Originally called Blackstone Rangers, they are also known as the Black P. Stone Nation (BPSN).

BS – Bomb Squad: An Atlanta, GA area street gang

BSL - Brown Side Locos: A Hispanic street gang that is active in California and Georgia.

BTK - Born To Kill: A Vietnamese-American street gang founded in New York in the 1980s.

D&D – Down and Dirty: An Atlanta, GA area street gang

D4L – Down 4 Life: An Atlanta, GA area street gang

DFB – Dem Franchise Boyz: An Atlanta, GA area street gang

DMI - Dead Man Incorporated: A Caucasian prison/street gang founded in the Maryland prison system in the late 1990s.

DP – Da Posse: An Atlanta, GA area street gang

DSB - Down South Boys (Down South Boyz): A Florida street gang.

EPT - El Paso Tangos (Tango Blast): A Texas gang comprised primarily of Hispanics.

4CH - Four Corner Hustlers: An African-American street gang founded in Chicago, Illinois in the late 1960s.

F13 - Florencia 13: One of the largest Hispanic gangs in Southern California.

FSC – Fair Street Crips: An Atlanta, GA area street gang

FTRA - Freight Train Riders of America: A gang of individuals (hobos) who travel by rail boxcar. They are very active in the Northwest United States. Crimes include robbery and murder.

G-27 – The G-27: Formed in the Puerto Rico prison system. Members are referred to as “Insectos.”

GB – Gutta Boyz: An Atlanta, GA area street gang

GD - Gangster Disciples: An African-American street/prison gang founded in Chicago, Illinois. They have spread to numerous other states throughout the United States.

GKB - Gangsta Killer Bloods (Gangster Killa Bloods): A predominantly African-American street gang

GMB – Get Money Boyz: An Atlanta, GA area street gang

GMC – Get Money Crew: An Atlanta, GA area street gang

GS – Goone Squad: An Atlanta, GA area street gang

GSC - Grape Street Crips: A Southern California street gang.

GTO – GTO Bad Boyz: An Atlanta, GA area street gang

GTSN – Gangster Two Six Nation: An Atlanta, GA area street gang

HPL - Hermanos de Pistoleros Latinos: A Hispanic prison gang founded in the Texas prison system in the late 1980s; also known as Hermandad de Pistoleros Latinos.

HS – Hit Squad: An Atlanta, GA area street gang

HVK - Hidden Valley Kings: An African-American gang founded in Charlotte, North Carolina's in the 1990s.

IG – Imperial Gangsters: An Atlanta, GA area street gang

ISC – Insane Spanish Cobras: A Hispanic street gang founded in Chicago, IL

IVL - Insane Vice Lords: A Chicago African-American street gang.

LC - Latin Counts: A Latino street gang founded in Chicago, Illinois

LGF - La Gran Familia: A Hispanic gang alliance.

LHS – Lady Hit Squad: An Atlanta, GA area street gang

LRZ - La Raza (The race): A Hispanic gang.

MC - Mickey Cobras: An African-American gang founded in Chicago, Illinois.

MDC – Most Dangerous Click: An Atlanta, GA area street gang

MLD - Maniac Latin Disciples: A large, Hispanic street gang founded in Chicago, Illinois.

MOB - Men Over Bitches: A North Carolina street gang.

MOB – Member Of Bloods: An African-American street gang.

MOB - My Only Brothers: An African-American street gang in California.

MS – Murder Squad: An Atlanta, GA area street gang

MS-13 - Mara Salvatrucha: A transnational Hispanic gang that has spread to at least 42 states and approximately nine countries. They are described as America's most dangerous gang.

MW - Mandingo Warriors: An African-American prison gang founded in Texas in 1984.

NBCC - Nutty Blocc Compton Crips: A Southern California street gang.

NF - Nuestra Familia: A predominantly Hispanic prison gang with ties to the Norteños. The gang that was founded in the California prison system in the 1960s. Their main rival is the Mexican Mafia. In some areas they are now established on the streets.

NLR - Nazi Low Riders: A white supremacist gang founded in Southern California.

NS – Northern Structure: Believed to be a spin-off prison gang of La Nuestra Familia

PBS - Playboy Surenos: A predominantly Hispanic street gang found in multiple locations across the country. PBS 13, and PBS X3 are a couple of other tags associated with this gang.

RAC - Raymond Ave. Crips: A California African-American street gang.

SB – Soldier Boyz: An Atlanta, GA area street gang

SC - Spanish Cobras: A Hispanic street gang founded in Chicago, Illinois.

SCR - Simon City Royals: A predominantly Caucasian street gang founded in Chicago, Illinois.

SNM – Sindicato Nuevo Mexico (New Mexico Syndicate): The SNM is considered to be the most violent and most powerful of all of the Security Threat Groups within the New Mexico Department of Corrections.

SSC – South Side Crips: An Atlanta, GA area street gang

SUR 13 - Surenos – (Spanish - Sur means south; Sureños means southerner): Originated in Southern California as a street gang but has found its way into the prison system and has spread throughout many parts of the United States. Sureños are considered to be the soldiers for the Mexican Mafia prison gang. Blue is the gang's traditional color. The number 13 associates

them with the Mexican Mafia – the letter M is the thirteenth letter of the alphabet. They may also use XIII or X3.

3C – Triple Cross: An Atlanta, GA area street gang

3Ni – Trinitarios: Trinitarios started in New York City as a prison gang within the NY City Dept of Corrections and then the State DOC, during the early 1990s.

TB - Tango Blast: A street/prison gang based in Texas.

TM - Texas Mafia: A predominantly Caucasian gang founded in the Texas prison system in the early 1980s.

TRG - Tiny Rascal Gangsters: An Asian-American gang, also known as the Tiny Rascal Gang or the Tiny Rascals.

TS - Texas Syndicate: A prison gang, also known as Sindicato Tejano, was founded in the early 1970s in the California prison system. Their gang members are primarily Mexican-American.

UBN - United Blood Nation: Originated about 1993 at Rikers Island prison in New York. The UBN is now found in many parts of the east coast of the East Coast of the United States.

VL - Vatos Locos: A west coast street gang that has spread eastward and may be found in North Carolina, Georgia, and Maryland.

VL - Vice Lords: A large, mostly, African-American gang street/prison founded in Chicago that now has a national presence. They are also known as the Vice Lord Nation (VLN), Almighty Vice Lord Nation (AVLN), and Conservative Vice Lord Nation (CVLN).

WBP - Wetback Power: A Mexican-American street gang. Also commonly called Sinaloa Cowboys.

WBC – White Boys Click: An Atlanta, GA area street gang

YBB – Young Block Boyz: An Atlanta, GA area street gang

YBG – Young Block Girls: An Atlanta, GA area street gang

YC – Young Choppers: An Atlanta, GA area street gang

YD – Young Diplomats: An Atlanta, GA area street gang

YDC – Young Dangerous Click: An Atlanta, GA area street gang

YGC – Young Gunna Crew: An Atlanta, GA area street gang

YM – Young Mafia: An Atlanta, GA area street gang

YM – Young Money: An Atlanta, GA area street gang

YP – Young Posse: An Atlanta, GA area street gang

YPN – Young Paid Niggaz: An Atlanta, GA area street gang

YS – Young Squad, Atlanta: An Atlanta, GA area street gang

YSH – Young Squad Hoes: An Atlanta, GA area street gang

YSss – Young Squad Stay Strap: An Atlanta, GA area street gang

YSM – Young Squad Mafia: An Atlanta, GA area street gang

YT – Young Team: An Atlanta, GA area street gang

Source: Los Angeles County Sheriff Department

INMATE SOCKS USED TO ATTEMPT OR COMMIT SUICIDE INTRODUCTION:

Correctional Services and Custody Operations Divisions have seen a concerning number of inmates who have attempted or successfully committed suicide using socks. In these situations, the socks issued to inmates or purchased through commissary, have been altered by stretching and then fashioned into a noose type devise used for hanging.

TYPES OF INMATE SOCKS

Presently, there are three types of socks in circulation within the jail system:

- *Standard Sock* - This sock is issued to all inmates. It is a white knee high sock with a yellow band around the top. Unaltered, it measures approximately 18 inches, and stretched, it can measure up to 31 inches.
- *Commissary Purchased Sock* - This sock can be purchased through inmate commissary. It is a white tube type sock. Unaltered, it measures approximately 23 inches, and stretched, it can measure up to 43 inches.

- *Anti-Embolic Medical Stocking* - This sock/stocking is issued by Medical Services to inmates with certain medical conditions. They come in two different styles: calf high and thigh high. Unaltered, the “calf high” measures approximately 19 inches, and stretched, it can measure up to 42 inches. Unaltered, the “thigh high” measures approximately 31 inches, and stretched, it can measure up to 65 inches.

AWARENESS

While conducting security checks or searches, be aware that any altered piece of inmate clothing, including socks, is considered contraband and should be confiscated. If you suspect that an inmate may be contemplating suicide by altering clothing or other items, make sure the inmate immediately receives proper medical attention.

Source: Los Angeles County Sheriff Department – Correctional Services Division, Custody Operations Division, Custody Support Services Informational Bulletin #2009-10

CELL PHONE TASER: On 09/02/21, while conducting an arrest on a traffic stop, District 4 members seized a taser disguised as a cellular phone. A small ‘ON’ switch was located on the side of the phone. When the centre button on the phone was pressed, a spark between two probes on the top of the phone was initiated.



The suspect indicated he purchased the taser on Ebay approximately one year ago.

Please keep this device in mind when conducting searches

Source: Calgary Police Service District 4 Office – Case #09062581

XERO'S EBOARD NEO: Xero technology has just announced their release of a new motorized skateboard that is controlled by a remote control. One of the remote control designs includes a remote in the shape of a gun. The new eBoard Neo goes an average of 14 miles per hour, 0 -20 in 4 seconds and has a contemporary wood finish. Please be aware of this new gun look-a-like remote.



Source: Seminole County Sheriff's Office

“DRY ICE” BOMBS: Clarkstown Police is investigating an incident of several “dry ice” bombs that were detonated at approximately 2330 on November 18th in the Prospect Street commuter lot, located directly behind the Nanuet Post Office (access is alongside the west wall of the Post Office). CPD received numerous calls reporting shots fired in the area.

Several youths were observed in the lot by a witness from a distance away immediately after the devices activated. Upon CPD arrival, no persons were found in the area. Officers located several devices that had exploded, but they also located 3 additional devices that had not yet exploded. The RC Sheriff's Ordinance

Disposal Unit responded and deactivated those devices.

These devices are easy to make and have become popular with youths due to active interest on the Internet. A dry ice bomb is made from a container (typically a plastic bottle), water, and dry ice. The bottle is filled about quarter full of water, some dry ice is added, and the container shut tightly. As the solid carbon dioxide warms inside a bottle, it transforms to a gas. The pressure inside the bottle increases as the quantity of gas increases with limited room to expand. Rupture will occur when the pressure inside the bottle exceeds the strength of the plastic. Bombs will typically rupture within 30 seconds to 30 minutes, dependent largely on the temperature of the air outside the bottle. A dry ice bomb may develop a frost on the bottle exterior prior to explosion. After explosion, a dry ice bomb will appear to have shattered, usually with the overall shape of the device intact. Dry ice bombs are most commonly used on their own to simply make a blast.

Devices that have not exploded are extremely dangerous. Most are contained in plastic bottles; however glass bottles have sometimes been used. They can literally explode at any moment. Also, any movement or shaking of a bottle may accelerate the reaction. Impact injury could occur from shrapnel, as well as auditory damage to one's hearing. All officers must use necessary precautions when encountering one of these devices.

Information learned to date show that at least 3 youths were present in the commuter lot. Description shows one youth wearing dark pants and a white shirt, no further as the witness was a long distance away. No vehicles were observed by the witness. No video of the location has been found from the lot or adjacent businesses. It is believed that the Dry Ice was purchased at American Compressed Gas, Route 304 Bardonia. They are the only registered supplier in Rockland County. The Dry Ice wrapper recovered from the scene has been identified as being the same style and type as used by ACG.

Reference complaint number: 09-30322

Source: Clarkstown Police - Detective Bureau 20 Maple Avenue New City, NY 10956 (845) 639-5840 or 5800; FAX (845) 639-5924

CONCEALMENT METHODS: US ARMY FLAG PATCH (WORN ON ACU UNIFORMS OVERSEAS): ACU Patch contained the following items: Handcuff Key, Bobby Pin and other metal pieces.



Source: Reagan National Transportation Authority

SURVEILLANCE TOOL: Compact Wireless 360 Degree Display System Eye Ball R1 is a compact wireless 360° mobile display system, designed to be used in tactical operations where law enforcement personnel need to see the situation before entering a building, floor or room. The Eye Ball R1 is rugged allowing tactical users to roll, toss, lower or throw it as applications demand. ODF's Eye Ball R1 gradually scans the scene to cover 360 degrees, transmitting the image and audio



from the scene, in real time, via wireless communication to remote and mobile display unit. Each sensor is packed in a hand-held durable ball, which is designed to be thrown to remote and potentially dangerous locations, without exposing the operators to the danger. The Eye Ball can sustain shocks and vibrations and other harsh environmental conditions. The Eye Ball R1 transmits streaming video and audio to a Personal Display Unit (PDU) that enables display of the image received from the Eye Ball, as well as control of the rotation direction of the sensor. Advanced versions of the Eye Ball include automatic video motion detection on the monitor. The Eye Ball R1 can quickly be attached to a pole providing visibility into ceilings and attics. Its near-infrared capability is essential for night or dark operations.

Source: Peel Regional Police

KEY KNIFE: This is being sold as a Christmas gift this year and is being sold online for \$25. Barely larger than an ordinary key, this German made pocket knife will easily slip on a key chain.



Source: <http://www.garrettwade.com/product.asp?splid=SPLID01&pn=02B05.01&bhcd2=1259331743>

OFFICIAL UNIFORMS USED IN MULTIPLE RECENT ATTACKS: Operatives in three attacks in Pakistan in October 2009 used official uniforms to gain access to protected and heavily fortified facilities. Reporting indicates that insurgents in Afghanistan and Pakistan have previously used official uniforms to disguise themselves as military or police personnel to blend into surrounding high-security environments.

- On October 15, approximately 25 terrorists dressed in police uniforms simultaneously attacked three law enforcement buildings in Lahore. Three teams of operatives assaulted two training centers and the Federal Investigative Agency building using small arms, grenades, and unspecified explosives.
- On October 10, terrorists wearing military uniforms attacked the Pakistani Army's General Headquarters (GHQ) compound using small arms and grenades. They killed security guards at the entry and proceeded to the GHQ building where they regrouped and continued their attack. The use of official army uniforms may have confused responding forces, allowing the attackers to take hostages that resulted in a 20-hour standoff that was resolved when Pakistani Special Forces stormed and regained control of the building.
- On October 5, a suicide operative detonated a device containing 16 pounds of explosives in the lobby of the United Nations World Food Program office in Islamabad, killing five and injuring eight. The bomber reportedly was not searched when he entered the facility, likely because he was wearing an Afghan Frontier Corps military uniform.

Comment: DHS is unaware of any credible intelligence indicating similar attack planning is ongoing in the United States. Local law enforcement in several jurisdictions, however, have reported incidents involving the theft of military and police uniforms, equipment, and official vehicle license plates. This type of activity could indicate preoperational attack planning, although we are not aware of any terrorism nexus to the thefts. DHS encourages law enforcement and security officials to be vigilant in identifying and reporting suspicious use of official credentials and uniforms and to ensure these items are properly secured from theft. Potential Indicators of individuals using stolen or counterfeit uniforms or equipment are provided below. The presence of one or more of these indicators does not necessarily indicate a pending attack, but may indicate the need for further investigation or an increase in security measures.

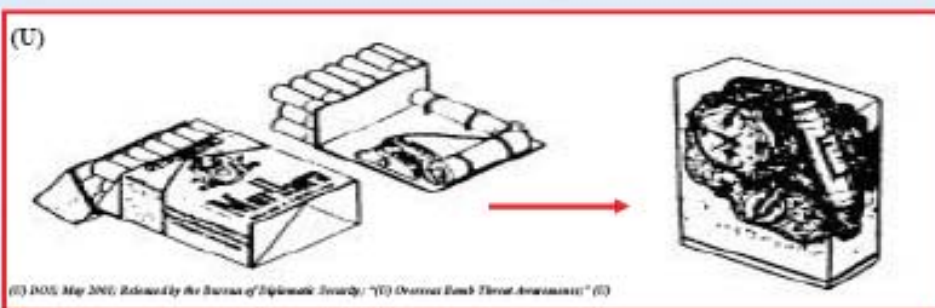
- Theft of emergency, military, law enforcement, or other official uniforms or equipment.
- Illicit use of official or counterfeit uniforms, materials, or vehicles to facilitate entry to registered sites or allow unauthorized individuals to act in an official capacity.
- Individuals in official looking uniforms who do not conduct themselves according to protocol (lack of military bearing or unfamiliarity with common military and security terminology and rank).
- Improper use or wear of official uniforms (missing patches, unusual uniform colors, sloppy or ill-fitting uniform, or incorrectly worn insignia).

Source: DHS Office of Intelligence Analysis Note



BE ALERT:

(U//FOUO) Seemingly harmless cigarette packs or small tins (such as the ones pictured below) have been used to conceal explosives, weapons, or drugs.



(U) Box of cigarettes used to disguise improvised explosive device (IED)



(U) Mock-up cigarette pack jammer

(U) Metal tin used to conceal electronics

(U) Mock-up cigarette IED

(U) Small Package Concealment Method



Transportation
Security
Administration

Prepared by TSA-Office of Intelligence
November 2009

UNCLASSIFIED//FOR OFFICIAL USE ONLY

PSTR-81553-2009-11-25

CRIMINAL INTELLIGENCE

FEDERAL INMATES ADOPT SOVEREIGN CITIZEN FRAUD TACTICS: At least two federal inmates attempted to defraud the Federal Bureau of Prisons by mailing fraudulent checks to National LockBox, a depository for inmate commissary funds, according to FBI reporting. This technique is consistent with previously reported sovereign citizen extremist tactics. Two identified inmates at Oakdale, Louisiana Federal Correctional Institution attempted to make fraudulent National LockBox deposits in September 2009. The counterfeit certified bank drafts, in the amounts of \$3,000 and \$5,000, were purportedly drawn on the inmates' trust accounts at the Federal Reserve Bank of Atlanta, Georgia. Personnel at National LockBox determined the checks were fraudulent and did not transfer the funds.



(U) Fraudulent Check
Passed by Federal Inmate

Comment: The FBI assesses the inmates likely learned sovereign citizen fraud tactics while in prison; both were originally incarcerated for crimes unrelated to sovereign citizen extremism. Though this tactic was uncovered in the federal prison system, the FBI anticipates inmates will likely share the tactic and encourage its wider use.

Source: FBIHQ – Domestic Terrorism Strategic Operations Section and FBIHQ – Counterterrorism Analysis Section.

INTERNET SCAM: FAKE VERIZON "BALANCE CHECKER": Cyber-criminals have started preying on Verizon Wireless customers, sending out spam e-mail messages that say their accounts are over the limit and offering them a "balance checker" program to review their payments. The balance checker is actually a malicious Trojan horse program. Victims who download the software open up a back door to their computer, where more malware can be downloaded from the Zbot botnet, which is known for stealthily lifting online banking credentials and emptying accounts. Recently, the U.S. Federal Bureau of Investigation said this type of financial fraud has removed \$100 million from U.S. bank accounts.

Source: www.computerworld.com

JUGGALOS AND JUGGALETTES: The Juggalos and Juggalettes (females) have a heavy presence on the East Coast and rapidly growing across the US with members in the thousands. They are followers with a true addiction to the Insane Clown Posse (one of the most hated bands in the world) and have based an entire life style around them. They do not jump in to a gang, but they are very dedicated to the Insane Clown Posse and each other. They claim no violence, but this is not true. The make-up of this group is mainly Caucasian. They have lines of clothing, jewelry, paraphernalia, etc. Most that claim Juggalo or Juggalette will have tattoos. They also follow other bands such as the Dark Lotus, Twiztid, Anybody Killa, Jumpsteady, Psychopathic Rydas, etc. These are all violent, sinister and vulgar rap/rock groups. The Insane Clown Posse began in the early 90s out of Detroit, giving themselves the identity of clowns to better fit in while preaching the messages of the “Dark Carnival.” The Juggalos can be identified by heavy clown make-up (sadistic wicked type faces and jester style), tattoos, clothing, and specific music possessions. The hatchet man (tattoo above) is the most common tattoo as it is the symbol of the Insane Clown Posse record label, “Psychopathic Records”. The hatchet can be seen in numerous colors. They also tattoo other music groups they follow - “ICP”, “Dark Lotus” (tattoo above), etc., along with many other types of tattoos. They wear dark clothing, but do like to also dress in bright clown colors, dye their hair in bright colors, and wear Mohawks. They like to stand out and be noticed. They tag areas with “ICP”, “Dark Lotus”, etc. They also have their own hand signs. Excerpt from internet: “A Juggalo is someone who doesn't give a f_ _k what people think about them. They have entered the world of the Dark Carnival and Insane Clown Posse because they themselves have been considered clowns, buffoons, idiots, and freaks. Being a Juggalo reflects an entire lifestyle and state of mind... it is something that is impossible to define, even for a Juggalo. To understand what a Juggalo is, you must truly be a Juggalo.” The ICP also references the “Dark Carnival” in their lyrics, which to all Juggalos is “GOD.” It is the ultimate heaven for Juggalos, “where they will experience paradise and never have to worry.”



Source: Florida Department of Corrections – Bureau of Classification Security Threat Intelligence Unit, Monthly Gang Intelligence and Activity Report, November 2009



FINANCIAL FRAUD SCHEMES INVOLVING SSNS WITH 586 PREFIX: Immigration and Customs Enforcement (ICE) has provided OI with information concerning the counterfeiting and alteration of People's Republic of China (PRC) passports being used in conjunction with legitimately issued Social Security Number (SSN) cards beginning with the

prefix "586" in order to commit financial fraud schemes. According to information from ICE, Asian-organized identity theft rings are using these identification documents to assist individuals in obtaining state driver's licenses or identification cards. All three forms of identification documents are comprised to create "identity sets", which are sold for anywhere between \$1,200 and \$3,500.

Not all individuals using these "identity sets" are of Chinese descent, as many individuals associated with past fraud schemes were actually Korean or Indonesian nationals entering the U.S illegally. In addition, many of the names appearing on both the SSN cards and PRC passports can easily be interchangeable between genders. The names can also be used as either a first or a last name. These types of fraud schemes have been identified in **Chicago, Dallas, New York, Los Angeles, and Las Vegas.**

Background

SSN cards containing the prefix "586" are issued to residents and citizens/nationals of American Samoa, Guam, the Philippines, and the Commonwealth of the Northern Mariana Islands (CNMI). CNMI's largest island and capital is Saipan; it is also the location of the Commonwealth's Social Security office.

Saipan's economy primarily depends upon U.S. funding, tourism, and the garment industry. During the garment industry's peak period (mid to late 1990's) more than 17,000 non-citizens worked in the garment factories in Saipan. The majority of these workers were Chinese nationals. According to 2000 U.S. Census Bureau data, more than half (approximately 56%) of CNMI's population were non-citizens.

The early 2000's brought about a change in the trade laws, which coincided with the decline in the garment industry in Saipan, and a reduction in the need for garment factory workers. Without the garment industry, there is no longer a need for visiting garment factory workers to remain in Saipan, and they must return to their native countries. Therefore, these workers no longer require an SSN card. These SSN cards are then acquired at some point in time and are subsequently shipped to the United States for sale to fraud rings specializing in identification documents.

Related Investigations**OI New York Field Division Case # NYC-09-00013-T**

The OI New York Field office opened a case on 10/10/08, upon notification of the Department of Homeland Security's (DHS) seizure of a Federal Express (FedEx) package. The FedEx package, containing Social Security cards and photocopies of Chinese passports, was selected for random inspection by the DHS Customs and Border Protection (CBP). Its origin was Saipan, Northern Mariana Islands (sent from a manager of a defunct garment factory), and its destination was Flushing NY. The occupant of the delivery address was questioned and revealed that he paid human smugglers \$30,000 to enter the U.S. and an additional \$800 for an Illinois State driver's license. The SSN cards and passports were used as a means of identification to obtain driver's licenses. Eventually all of the documents were used to commit financial fraud. This case was declined for prosecution.

OI Dallas Field Division Case #DAL-07-00080-P

On 03/01/07, the OI Dallas office was contacted by ICE for assistance with an investigation. The CBP intercepted a package shipped from the PRC containing two counterfeit PRC passports. The package was scheduled for delivery to a Texas address. The occupant of the Texas address admitted that the passports were part of a fraud scheme to obtain credit, and the scheme included the use of SSN cards (some with a 586 prefix) and fraudulently obtained driver's licenses. The subject pled guilty to Access Device Fraud and was sentenced to 57 months' imprisonment, two years' supervised release, and ordered to pay restitution in the amount of \$180,699.

ICE Los Angeles and Las Vegas Investigations

The Department of Homeland Security (DHS) ICE Forensic Document Lab is currently conducting intelligence research on counterfeit Chinese passports in support of on-going ICE investigations that relate to the use of counterfeit passports for financial crimes in Los Angeles and Las Vegas. According to ICE Intelligence, counterfeit Chinese passports have been seized by CBP at mail facilities in several locations, mostly on the west coast, since the mid-2000's. Further ICE Intelligence advised that many of the subjects who are involved with the counterfeit passports in the U.S. are associated with financial crime operations that involve the use of alias identities based on SSNs issued in Saipan and linked to the FBI Chicago's "Operation Paper Mountain".

FBI Investigation "Operation Paper Mountain"

"Operation Paper Mountain" is an ongoing investigation that began in Chicago, IL, in 2007, after the merger of two separate and independent investigations by the Chicago Police Department and the FBI. The investigations noted that between 2003 and 2008, 15,666 Illinois State driver's licenses and state identification cards were issued to individuals using SSNs

beginning with "586". Those numbers are a distinct contrast to the 787 cards that were issued during a much larger time frame – 1970 through 2002. Additional investigation identified a crime ring that had been selling fraudulent identification documents, including counterfeit or altered PRC passports, for at least five years. In February 2009, 19 individuals, including two (2) former Secretary of State (driver's license issuing agency) employees, were arrested and charged with conspiracy to produce fraudulent identification documents. *(Note: The OI Chicago office has conducted SSN verification requests in support of this operation.)*

Conclusion

(U//LES) Based on current investigative information, there is no indication of enumeration fraud being committed against SSA. Original SSN cards appear to have been applied for in accordance with the immigration laws of the Commonwealth of the Northern Mariana Islands, at that time, and legally issued. *(Note: Effective November 28, 2009, under the Consolidated Natural Resources Act of 2008, DHS will be taking over the immigration procedures, and the Northern Mariana Islands immigration system will convert to U.S. immigration laws.)*

In furtherance of the Office of Investigations' mission to protect the integrity of the SSN, the Strategic Research and Analysis Division (SRAD) is continuing to work with ICE to collect intelligence and to track the misuse of SSNs with the "586" prefix, as well as any other trends that pertain to the misuse of an SSN in relation to financial crimes. OI Field Divisions are asked to report allegations or cases involving the misuse of SSNs with the "586" prefix, as well as any other similar fraud schemes, to SRAD.

Source: Social Security Administration - OIG Intelligence Brief, 13 November 2009

THE RISE OF THREATS AND ACTS OF VIOLENCE IN ANIMAL RIGHTS EXTREMISM: 2003-2008: Between 2003 and 2008, animal rights (AR) extremist threats of violence increased steadily and significantly, making up more than one quarter of all AR extremist criminal activity. Violent acts, which made up seven percent of AR extremist criminal incidents during those years, increased primarily through acts of arson and attempted arson, but also included bombings, physical altercation, and the use of BB/pellet guns. However, none of the reported incidents in the United States resulted in serious injury. Non-violent acts such as theft, cyber crimes, harassment, trespassing, and vandalism comprise the remaining majority (67 percent) of AR extremist criminal incidents.

The increase in threats and acts of violence occurred after a period of decline in violence and coincided with AR extremists' fluctuating efforts to shut down Huntingdon Life Sciences (HLS), renewed interest against the fur industry, and emerging campaign to target university researchers. The FBI assesses with high confidence it is very likely AR extremists will continue

to make threats and commit acts of violence as part of a continued effort toward animal liberation.

AR extremists commit criminal actions in order to defend animals and intimidate those perceived as exploiting animals. The ideological framework behind the Animal Liberation Front (ALF), with which many AR extremists claim affiliation, includes a set of publicly stated guidelines admonishing adherents to “protect all forms of life, human and non-human.” The increase in threats of violence, the continued and increasing acts of violence, and the violent rhetoric challenge this restriction on physical harm to humans and increase the potential for human injury.

AR extremists will likely continue to use violent acts and threats of violence to further intimidate their victims. Statistical calculations forecast that, based on the rate of increase during the last six years, the trends for the next two years will continue to increase, and the threats and acts of violence in 2010 will almost double the number that occurred in 2008. However, with continuing efforts by law enforcement and the increased penalties and expansion of scope in the Animal Enterprise Terrorism Act, it is unlikely criminal activity will increase to the extent suggested by statistics.

AR extremists generally advocate protecting life and focus their campaigns on intimidation of victims with no intent to cause injury. Some AR extremists, operating in small cells or as lone offenders, however, may use violence which results in harm to individuals, whether intentionally or not. Some AR extremists in the United States may be influenced by AR extremists in the United Kingdom where violent acts such as assaults and bombings have historically been more common and have resulted in several injuries. An intentional act of violence against a human target would likely instill fear in other previous or potential victims of AR extremism, as well as cause the AR extremist movement to splinter between those individuals advocating the protection of life and those who may wish to cause harm. We assess with high confidence it is unlikely the ALF, however, will change its guidelines which admonish adherents to protect all forms of life.

FBI Newark Comment. Considering the past level of animal rights extremist activity in New Jersey, the above analysis is noteworthy and insightful about the types of criminal activities that can be expected from AR extremists. Although AR extremist activity has declined somewhat since the 2006 conviction in a New Jersey federal court of six Stop Huntingdon Animal Cruelty (SHAC) members, AR extremists remain committed to shutting down Huntingdon Life Sciences (HLS), a major animal research facility headquartered in Franklin Township New Jersey.

Source: FBI Intelligence Assessment, 12 November 2009 (UNCLASSIFIED).

SECURITY RESPONSE OF ANIMAL RIGHTS EXTREMISTS FOLLOWING THE ARREST OF AN ASSOCIATE IN LATE SEPTEMBER 2009: Three animal rights extremists initiated several security techniques following the arrest of associate and subsequent interviews of other extremists. The extremists, USPER 1, USPER 2, and USPER 3 advised they purged the names and telephone numbers of other members and associates from the memory of their cell phones. USPER 1 planned to get rid of a personal computer because of previous communications made on a social networking Web site (NFI). USPER 2 also deleted a personal Web page on the same social networking Web site. USPER 3 intended to disassociate with USPER 1 and USPER 2. USPER 3 also indicated that any subsequent discussions about the arrest and interviews should be held away from any animal rights extremists' residences.

Source: FBI IIR 4 201 0998 10 (UNCLASSIFIED).

LIQUID MARIJUANA: Liquid Marijuana, described as a dark green mixture of alcohol and marijuana was recovered during a search warrant that was executed in Brooklyn, NY (62nd Precinct). The liquid marijuana was seized in 8 mason jars and 3 Poland Spring bottles. The mixture was allegedly being sold at a price of \$120 for approximately 16 liquid ounces. The perpetrator made statements that he made the mixture at home. He revealed that he soaked the marijuana in 160 proof vodka and lemon vine for 2 weeks. He then placed the liquid in a microwave to heat it, filtered the mixture and then packaged it to be sold. Prior to drinking, individuals would mix it with a flavored drink such as Kool-Aid. To generate substances such as "marijuana honey hash oil" and "marijuana butter" it is necessary to heat the marijuana plants that is coated in isopropyl alcohol for an extended time. Alcohol and the heat acts to break down the THC resin from the marijuana plants into liquid form. Alcohol may cause cook top fires if the heating source comes into contact with the flame.



Various websites offer instructions and recipes for “liquid marijuana” mixtures. One such website is as follows: http://www.truthtree.com/thc_extract.shtml. An excerpt from this website describes in detail, a technique of extracting the essential oils from hemp. The final product will be a dark, oily liquid that contains 70+% pure THC. The steps require nothing more than simple, easy to find materials and a little time.

Source: NYPD Intelligence Division – Narcotics Intelligence Unit, Intelligence Alert, 20 November 2009

LOGOS ON PACKAGES OF COCAINE: In recent months, the logos on narcotics packages seized in the U.S. included: a Black Spider (Viuda Negra/Arania Negra) and a Yellow Horse Head (Cabeza de Caballo Amarillo). Of hundreds of packages in each shipment, only one or two had the logo.

- July 7, 2009, Phoenix, Arizona, Black Spider logo on cocaine kilo packages
- May 15, 2009, Tilden, Texas

'222' ; impressed on cocaine bricks



Black Spider on cocaine brick



- Logos on packages of cocaine seized in Dominican Republic and Puerto Rico



- Other logos on seizures in Dominican Republic and Puerto Rico
 - Black Spider logo inserted into kilo package of cocaine
 - A '1A' in a black star in a red circle on white paper
 - An '8a' signifying Ochoa

- A bowling pin
- A plain blue square logo
- 'ZX1000' in white letters on one kilo package of cocaine
- A black 'V' logo (on heroin packages)
- Other logos on seizures in Dominican Republic and Puerto Rico

Playboy Bunny



Indian Head and '777'



Kangaroo and 'R A M'



Butterfly and '777'



Various designs



Comment: DEA maintains a database of logos from seized drug shipments. For questions, comments, information, or logos you wish to submit, contact program managers Cheryl Amado; 202-307-5036 or Carolyn Brown; 202-307-8375. For a list of street terms and definition of the associated drug, please contact the Office of National Drug Control Policy (ONDCP). <http://www.whitehousedrugpolicy.gov/streetTerms/byalpha.asp>.

Source: Arizona Department of Public Safety Arizona Drug Intelligence Task Force/HIDTA – Investigative Support Center Intelligence Bulletin

CAMERA DISGUISED AS CAN OPENER: Hidden camera integrated into an everyday tool, a can opener. The can opener is fully functional. The black and white version of the camera can also be used to generate good quality video in total darkness, which the color version compromises on.



Source: <http://www.spyreview.co.uk/2008/12/25/a-hidden-camera-disguised-as-a-can-opener/>

“DISGUISED” USB THUMB DRIVE (KEY): From the vendor: “With the LaCie iamaKey, inventive storage meets data protection. The key-shaped design is functional and memorable, and the protection that the LaCie iamaKey offers makes it extremely reliable. Best of all, with its 4GB, 8GB, and 16GB models, you can fit an enormous amount of data in a small flash drive.”



Comment: This is another example of a data storage device in a form factor which could easily be overlooked. IT security staff and officers conducting searches should be aware of the possibility that a key ring contains relevant data. SCIIC-South Carolina Law Enforcement Division

Source: <http://www.lacie.com/us/products/product.htm?pid=11225>

CONTINUED CONCEALMENT OF DANGEROUS AND CONTRABAND ITEMS WITHIN TOYS:

This bulletin is intended to alert Federal Protective Service (FPS) law enforcement and contract security personnel to the potential for terrorists or others with criminal or nefarious intentions to utilize children's stuffed "Teddy Bears" and other toys to conceal dangerous and/or contraband items to avoid detection by law enforcement and security. This tactic increases the risk to federal buildings and employees since the presence of children's toys and stuffed animals do not generally raise a security concern and can easily be overlooked by security personnel if protocols are not followed. Many of our federal buildings offer daycare services or are frequented by families with young children, potentially increasing the likelihood of a terrorist or criminal attempting to exploit this potential concealment method.

BACKGROUND

On October 8, 2009, three men were indicted on federal charges for attempting to smuggle 11 kilos of cocaine wrapped and stuffed in boxes of Nerf and Hot Wheels toys in their baggage while boarding a flight from Seattle to Anchorage, Alaska.



On August 18, 2009, an examination of air cargo at San Juan International Airport destined to New York revealed approximately 5 pounds of cocaine concealed within stuffed teddy bears.

On January 2, 2009, airport security screeners in San Antonio, Texas discovered a stuffed teddy bear concealed within passenger carry-on baggage. The teddy bear was wrapped in wires which were connected to several plain brown wrapped packages, which resembled a suicide vest. A small note written in Arabic stating "Death by Chocolate," was attached to the bear. Following an evacuation and a law enforcement investigation it was determined that this bear was manufactured by a co-worker for amusement and the packages actually contained chocolate bars.



On December 28, 2008, airport security screeners in New York detected two rubber ducks that had altered with wires, switches and a circuit board. One of the ducks had visible wires wrapped around it, while the other duck was cut open and contained the circuit board as well as the switches. The passenger indicated the items created an audio device and were part of a school project.

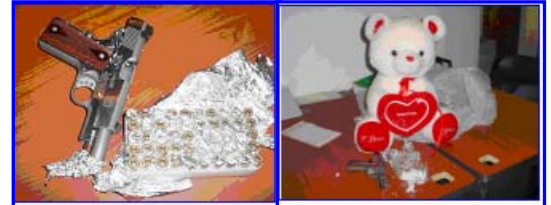
On October 20, 2008, Israeli police and customs service arrested two subjects who were attempting to smuggle cocaine into Israel from South America by concealing it within various toys.



In February 2008, an explosive device concealed within a soft toy was discovered by police in Southern Russia on a passenger bus.

In May 2007, airport screening personnel in San Juan, Puerto Rico discovered a knife concealed within a doll. Further investigation revealed the doll is sold on the street in San Juan.

In 2006, the U.S. Customs and Border Protection have recorded approximately 11 seizure cases involving the use of "Teddy Bears."



On December 4, 2006, Atlanta Police recovered a .45-caliber handgun and a box of ammunition concealed inside a "Teddy Bear" left unattended in the public area of Atlanta Airport.

On November 24, 2006, a joint Israeli operation involving Shin Bet and paratroopers discovered an explosive lab in Nablus, which is within the Palestinian territory on the West Bank. During a search of the lab, the forces found several "Teddy Bears" with wires protruding out of them. It is believed these toys were being fitted with explosives. Also discovered in the operation were other items that were used to conceal, produce or detonate explosives. This includes belts made from cloth, a hollow coat, hollow pipes, a hollow gas tank, batteries, light bulbs with fixtures and a quantity of hydrogen peroxide.



On August 3, 2004, a passenger was detained at a security checkpoint in the Orlando International Airport (OIA) after an X-ray machine revealed a pocketknife concealed within a stuffed "Teddy Bear."

On February 27, 2004, Modesto, California Police conducting a traffic stop discovered 28 one-ounce packets of heroin worth about \$50,000 concealed within a large "Teddy Bear." The operator exhibited suspicious behavior during the stop, which led officers to the discovery of the contraband.

On September 12, 2003, United States Customs and Border Protection (CBP) Officers seized a half-pound of heroin at the El Paso port of entry. The drugs were concealed in a stuffed animal that was being carried by a 25-year-old male. The courier displayed suspicious behavior during the encounter.

On July 12, 2003, a family was stopped at the security checkpoint at Orlando International Airport (OIA) after a security screener using an X-ray machine detected a gun (derringer)

concealed within a “Teddy Bear” in the possession of a child. The family indicated that a person at the hotel they were staying at had given the toy to the child.



On June 29, 2003, the Sunday Times (London) reported that prosecution witness David Rupert testified against Michael McKevitt, who was accused of directing terrorism and being a member of the Real Irish Republican Army. Rupert claimed in court testimony that he was told how to ship the explosives to Ireland concealed in teddy bears, “jump ropes” (skipping ropes) and radios.

In August 2000, local California law enforcement arrested a suspect who was carrying a handgun that was concealed within a “Cookie Monster” stuffed toy. The back of the toy was closed using Velcro. Other similar toys also containing weapons and contrabands had also been recovered.

ANALYSIS:

While the FPS Threat Management Division has no knowledge of terrorists or others planning to conduct attacks within the United States using “Teddy Bears” or other items to conceal dangerous weapons and/or contraband, this method of concealment is viable and is actively being used by terrorists and others in various parts of the world. Convicted terrorist Ramzi Yousef, who assisted in the planning of the 1993 attack on the World Trade Center, was found to have used children’s toys to conceal bomb components following his 2005 arrest in Pakistan.

Since many federal office buildings do have daycare facilities operating within them, it is possible that terrorists or others could exploit the presence of the daycare by using this concealment method as a ruse to transport dangerous weapons or contraband into federal facilities.

Although this document primarily addresses the use of “Teddy Bears” and other children’s toys as a concealment method, terrorists and other criminals have utilized other concealment methods in the past to transport contraband and other hazardous devices in an effort to avoid detection by law enforcement or security. These methods include the use of prosthetics, false compartmented books, canes, shoes, belts and other clothes, false bottom soft drink cans and other containers, and many other items. Therefore, the concealment method used is only limited by the creativeness of the courier.

FORCE PROTECTION RECOMMENDATIONS:

This potential concealment method highlights the continuing need for vigilance on the part of law enforcement and security personnel. All FPS officers and contract guards should continue to follow established national policies and local procedures to help ensure the safety of federal facilities, employees, and visitors. This includes using available technology (e.g., x-ray machines and magnetometers) and physical inspections of items being brought onto federal facilities based on established protocols, as well as continuous visual observation of all individuals and vehicles located on or adjacent to federal property.

Since even harmless looking items may be used to concealed explosives or other contraband, it is critical that personnel maintain constant vigilance and pay attention to other indicators of danger.

Any suspicious or unusual behavior—including but not limited to evasiveness, nervous mannerisms, excessively heavy or loose clothing that is “out of place” for the surrounding environment, or not responding to commands or greetings—may warrant closer scrutiny during the screening process. Security personnel should report anything out of the ordinary to FPS or local law enforcement in accordance with the standard operating procedures at their assigned facility.

Source: U.S. Department of Homeland Security Federal Protective Service Threat Management Division Date: 11/23/2009, Report Number: HQ-IB-016-09



ITEMS of INTEREST

EMERGENCY SERVICES PLANNING AND RESPONDING TO SHOOTINGS INCIDENTS: Recent shooting incidents, especially those receiving national attention, reinforced the necessity for all local, regional, state, and federal resources to plan for and prepare to respond to these events. Considering this need, the Emergency Management and Response—Information Sharing and Analysis Center (EMR-ISAC) researched the free “Mass Shooting: Planning and Response for Fire and EMS” presentation. The program states that a rapid, safe, and successful response to these situations requires deliberate planning and preparation. The PowerPoint slide presentation provides information and basic tools for first responders, emergency managers, school systems, and other officials to assist in the development or assessment of a multi-agency mass shooting response plan. One slide lists the following as the purpose of the program:

- Familiarize trends in active shooter/mass shooting events.
- Assist in understanding the nature of current and emerging threats.
- Suggest resources, plans, and training that will minimize the loss of life.

The EMR-ISAC noted the program includes the following areas:

- Multi-agency planning
- Crisis response kit
- Deterrence environment
- Command post
- Response tactics
- Scene assistance

In lieu of the PowerPoint material, a free 45-minute video is available. According to their web site, the Firefighters Support Foundation provides a program detailing the actions that fire and EMS agencies can take to prepare themselves for this all-too-likely event, and the actions they can take when the event occurs.

Source: EMR ISAAC INFOGRAM 45-09

STATE POLICE FORCES SHRINK: The number of highway patrol officers has shrunk in a dozen states in the past 13 years and failed to keep pace with population gains in others, leaving stretches of highways unpatrolled during late-night and early morning hours, a USA TODAY analysis of federal and state data finds. The shortages, which come as states battle billions of dollars in budget gaps, have forced places such as Oregon to cut down on 24-hour patrolling. Other states, such as Michigan, also have limited how many miles a trooper can drive per day. To get federal highway funds, states must assign some troopers duties such as truck safety and weigh stations, says Sheldon Greenberg of the Division of Public Safety Leadership at Johns Hopkins University. "They're not having troopers to do basic patrol work," he says. Greenberg says repeated cutbacks have some agencies at a breaking point. "Police agencies are digging themselves into a hole that will be very hard to get out of if it continues for too many years," he says. Florida, Georgia, Kansas, Kentucky, Maine, Maryland, Michigan, Missouri, Montana, Oregon, South Carolina and South Dakota have smaller state patrols than they did in 1995.

Source: South Carolina Information & Intelligence Center – Daily Information Bulletin # 218-09, 16 November 2009 / http://www.usatoday.com/news/nation/2009-11-15-troopers_N.htm?loc=interstitialskip

2009 HOMELAND TERRORIST PLOTS & ATTACKS: A TRANSPORTATION PERSPECTIVE

Plan to Launch Attack with Automatic Weapons

Plot Disrupted: October

Location: Massachusetts

Charge/Status: Conspiracy To Provide Materiel Support To Terrorists And Resources For Use In Carrying Out A Conspiracy To Kill, Kidnap, Maim, Or Injure Persons Or Damage Property In A Foreign Country and Extraterritorial Homicide Of A U.S. National/Arrested by federal authorities, investigation continues

USPERs Involved: Yes

Target: Shopping Mall

TTPs Resembled: November 2008 Mumbai financial district attacks

A Massachusetts man and his co-conspirators discussed their desire to participate in violent jihad against U.S. interests and radicalize others by distributing jihadi videos. The man and his co-conspirators discussed launching an attack at a U.S. shopping mall. Discussions included the coordination and weapons needed, and how to attack emergency responders. The plan was abandoned when they could not obtain the appropriate weapons. The man and two associates had traveled to the Middle East in 2002 and 2004 seeking to participate in terrorist training.

Attempt to Employ a VBIED Against a Federal Building

Plot Disrupted: September

Location: Illinois

Charge/Status: Attempted Murder of Federal Employees and Attempted Use of a Weapon of Mass Destruction in the United States/In custody, investigation continues

USPERs Involved: Yes

Target: Federal building in Springfield, Illinois

TTPs Resembled: Oklahoma City Bombing

Federal authorities arrested an Illinois-based USPER for attempting to detonate a vehicle-borne improvised explosive device (VBIED) outside the federal building in Springfield, Illinois. The man believed the United States is “at war with Islam.” The subject became radicalized in prison. He later expressed a desire to attend an overseas terrorist training camp and join the fight in Afghanistan, Somalia, or other locations. (*Source: FBI release, 24 September; Associated Press, 24 September; CBP release, 8 May 2008*)

Attempted Bombings and Simultaneous Surface-to-Air Missile Attack

Plot Disrupted: May

Location: New York City

Charge/Status: Conspiracy To Use Weapons Of Mass Destruction In The United States And Conspiracy To Acquire And Use Anti-Aircraft Missiles/Still in custody, investigation continues

USPERs Involved: Yes (4)

Target: Jewish Temple and Community Center, NYC & National Guard Base at Stewart Airport, Newburgh, New York Four men were arrested in New York City for a plot to detonate explosives near multiple targets, including a plan to simultaneously shoot Stinger surface-to-air missiles at military planes. The four men became radicalized while serving in prison, but lacked any formal terrorist training. One of the individuals stated he felt compelled “to do something to America” in retaliation for the war in Afghanistan. (*Source: BBC, 21 May; NY Daily News, 21 May*)

Man Potentially Involved in Explosives Manufacturing

Plot Disrupted: September

Location: Colorado; New York

Charge/Status: Conspiracy To Use A Weapon Of Mass Destruction, explosives/Arrested by federal authorities

USPERs Involved: Yes

Target: Possibly NY mass transit, hotels and stadiums

TTPs Resembled: London 2005 mass transit bombings

A 24-year-old Colorado man was indicted in New York for corresponding with a senior al-Qa'ida leader, and preparing for a potential attack against U.S. interests. The accused resided in Pakistan from August 2008 to January 2009, where he received "detailed bomb-making instructions." The USPER is alleged to have "purchased unusually large quantities of hydrogen peroxide and acetone products" —two ingredients that can be used in the manufacture of homemade explosives. Although the court documents do not reveal targets, the media reports that counterterrorism officials warned the New York mass transit system, hotels, and stadiums of an extensive plot to detonate backpack bombs. (Source: MSNBC; 18 September 2009; NY Daily News; 14 October, 2009; U.S. Department of Justice, 24 September, 2009; CBS News, 21 September)

Multiple Arrests of Possible Extremists

Plot Disrupted: August

Location: North Carolina; Virginia

Charge/Status: Providing Materiel Support to Terrorists and Conspiring to Murder, Kidnap, and Injure People Overseas/In federal custody, investigation continues

USPERs Involved: Yes (6)

Target: Quantico Marine Corps Base, Virginia

TTPs Resembled: 2007 Fort Dix, NJ

Federal agents arrested 6 USPERs and 1 foreign national for potential terrorist planning. The group had obtained maps and conducted reconnaissance of the Quantico Marine Corps Base in Virginia. Three members were indicted on separate charges of plotting to conduct a terrorist attack on the base. The suspects trained in the United States for terrorist operations and were allegedly willing to die as martyrs. The group's leader received training in Pakistan and Afghanistan, and had experience fighting in Afghanistan. The leader and two accomplices traveled to Israel in July 2007 to participate in "violent jihad," but, Israel denied them entry, which brought attention to the group. (Source: FBI release, 7 August; AOL News, 29 July)

Aspirational IED Attack on NY Transit System

Plot Disrupted: January

Location: New York

Charge/Status: Multiple, including Conspiracy to Murder U.S. Nationals/Pled guilty to federal custody, investigation continues

USPERs Involved: Yes

Target: NYC transit system

TTPs Resembled: Madrid train bombings

A suspected al-Qa'ida operative USPER admitted in federal court that, while in Pakistan, he trained with al-Qa'ida operatives and provided information about the New York transit system from his personal ridership experience. The USPER discussed the operations, communication equipment, and personnel of the Long Island Railroad (LIRR) and New York City transit systems to assist in planning an attack that would involve bombing New York City commuter trains. (*Source: Reuters, 23 July; Los Angeles Times, 23 July*)

Attempt to Detonate a VBIED Outside Iconic Building After Passing on Airport Site

Plot Disrupted: September

Location: Dallas and Ft. Worth, Texas

Charge/Status: Attempting To Use A Weapon Of Mass Destruction, VBIED/Pleaded not guilty, in federal custody, investigation continues

USPERs Involved: No

Target: Fountain Place, Dallas

TTPs Resembled: 1993 World Trade Center Bombing

Federal authorities in Texas charged a Jordanian citizen, who had met with undercover U.S. agents and discussed the possibility of conducting jihad against "the enemies of Islam." As part of pre-operational planning, the accused man surveyed the Dallas-Fort Worth International Airport, but passed on it as a target due to what he describes as "enhanced security". He eventually chose the Fountain Place office tower because it is one of Dallas' most recognized buildings. The FBI arrested the man after he attempted to detonate a fake vehicle-borne improvised explosive device (VBIED) that he had parked in the Fountain Palace's garage. (*Source: FBI Release, 24 September & April 16; Dallas Morning News, 26 September*)

Attack on Military Recruiting Station in Little Rock

Plot Disrupted: June

Location: Arkansas

Charge/Status: Pending, Murder

USPERs Involved: Yes

Target: Army-Navy recruiting station, Little Rock, Ark. A USPER conducted a shooting attack on an Army-Navy recruiting station in Little Rock with a semi-automatic rifle and pistol, among other weapons. One soldier was killed and one wounded. The USPER became the subject of an investigation after he traveled to Yemen in 2008, was arrested by Yemeni officials for using a false Somali passport, and was deported to the United States in January 2009. When interviewed regarding the shooting event, the arrested man stated he was angry about the killings of Muslims in Iraq and Afghanistan by the U.S. military. (Source: FOXNEWS.com, 2 June; CBP, 30 January; New York Times, 2 June)

USPER with Links to AQ Planning Attacks on Western Europe Targets

Plot Disrupted: October

Location: Illinois

Charge/Status: Conspiracy to Murder and Maim in a Foreign Country and Conspiracy to Provide Materiel Support to Terrorists/In federal custody; investigation continues

USPERs Involved: Yes (1)

Target: Various targets in Denmark, including newspaper building, military barracks, and train station

Two men were arrested for their alleged roles in conspiring to attack Western European targets. One of the men, a USPER from Chicago, conducted surveillance of potential targets during two separate trips to Denmark in 2008 and 2009. He reported his overseas surveillance to high-ranking members of al-Qa'ida and Lashkar-e-Taiba. The second man, a Pakistani native and Canadian citizen, helped arrange the USPER's travels overseas. The USPER allegedly possessed videos of the Danish Jyllands-Posten newspaper building, a Danish military barracks, and the interior and exterior of Copenhagen's central train station. The attacks reportedly would be in response to the published cartoons of the Prophet Muhammed in 2005.

Source: Department of Justice Release, 27 October; Reuters, 27 October; Chicago Tribune, 27 October

TERRORISTS CONTINUING MUMBAI-STYLE ATTACKS AGAINST DIVERSE TARGETS: Almost one year after the terrorist attack in Mumbai, India, militant Islamic extremists continue to conduct attacks internationally utilizing “Mumbai-style” tactics. For decades, terrorists have utilized tactics similar to Mumbai on lesser scale; although recently, terrorists using similar commando-style tactics have increased these types of attacks on diverse targets.

On November 26, 2008, ten members of the Pakistan-based terrorist group Lashkar-e-Tayyiba (LeT) landed in Mumbai, India, using an inflatable boat after traveling most of the way from Pakistan in a stolen fishing vessel. The militants were equipped with AK-47s, 9mm handguns, hand grenades, improvised explosive devices, and Global Positioning Systems (GPS). After arriving in India, the attackers split into groups and moved to assault multiple high profile targets simultaneously, while staying in contact via phone with LeT handlers in Pakistan.¹ Significantly, the selected locations had low levels of security and large numbers of people, maximizing the opportunity to inflict mass casualties.

Several tactics employed in the Mumbai attacks hold possible significance for U.S. law enforcement due to their potentially global applicability. These include selecting soft targets or targets of opportunity with large crowds, multiple operatives acting simultaneously, receiving real-time tactical direction from distant handlers, use of small arms and diversionary explosions, and hostage taking.

In Mumbai, terrorists launched coordinated attacks against high profile “soft” targets, such as hotels and a rail station with light security, and they specifically singled out foreigners. Since these attacks, terrorists using these commando-style tactics have continued to target hotels, rail systems and other “soft” targets of opportunity, such as marketplaces. Of note, attacks involving “Mumbai-style” tactics against decidedly “hard” targets, including military and law enforcement facilities, have also increased, almost exclusively in Pakistan.

Currently, there is no information indicating a specific threat regarding a similar type attack inside the United States. However, U.S. government officials have expressed concern about the possibility of an incident comparable to Mumbai occurring in the Homeland, because such operations require little money and involve materials (small arms and explosives) that are readily available in Western countries.

Source: NJ Regional Operations Intelligence Center (NJ ROIC) Counter Terrorism Desk ~ AE200910-876 November 18, 2009

SECRETARY NAPOLITANO MEETS WITH PRIVATE SECTOR CRITICAL INFRASTRUCTURE LEADERS, LAUNCHES NEW WEBSITE: Department of Homeland Security (DHS) Secretary Janet Napolitano today hosted the first in a series of roundtable meetings with private sector leaders to discuss critical infrastructure security and unveiled a new Web site designed to inform the public about the Department's critical infrastructure protection, readiness and resiliency efforts—part of her increased effort to heighten awareness about the importance of protecting America's vital assets, systems and networks over the coming weeks.

“Securing our nation's critical infrastructure is vital to maintaining the safety of communities across the country,” said Secretary Napolitano. “DHS is committed to working with federal, state, local, territorial and tribal partners, the private sector and the public to protect against threats to these assets, from cyber networks to drinking water.”

During the meeting with leadership from the Sector Coordinating Councils of the Energy, Nuclear, Water and Chemical Sectors, Secretary Napolitano highlighted her commitment to ensuring a more ready and resilient national approach to critical infrastructure protection, promoting vigilance, preparedness and risk reduction.

This session was the first of three Secretary Napolitano expects to hold with sector leaders. Two additional sessions are scheduled in the next two weeks focusing on public health, transportation, government facilities, information technology, communications, postal and shipping, national monuments and icons, manufacturing, and agriculture and food, emergency services, and defense industrial base sectors, among others.

Secretary Napolitano also unveiled a new Web site: www.dhs.gov/criticalinfrastructure designed to provide stakeholders and the public with easily accessible information about their role in safeguarding critical infrastructure and key resources (CIKR). The website features a link to the new CIKR Resource Center, which includes information about how to sign up for free Web-based seminars on the tools, trends, issues, and best practices for infrastructure protection and resilience; resources concerning potential vulnerabilities for chemical facilities; and details about the National Response Framework, which outlines guidance for all response partners to prepare for and provide a unified response to disasters and emergencies.

The Web site also provides information about DHS' ongoing CIKR efforts, including the National Infrastructure Protection Plan (NIPP), the U.S. Government's unified approach, coordinated by DHS, to ensure protection and resiliency of CIKR through partnerships with thousands of public and private members.

CIKR includes physical and digital assets, systems and networks that play significant roles in America's safety, economy and public health. Their incapacitation or destruction could debilitate the overall stability of the United States and threaten national security. (U) CIKR is comprised of 18 unique sectors—the vast majority of which is owned and operated by the private sector—including key areas such as food and water, manufacturing, energy, communications and transportation systems, and emergency services. DHS engages with these private sector partners via Government and Sector Coordinating Councils, which bring together state, local, tribal and private sector partners to coordinate security efforts.

For more information, visit www.dhs.gov/criticalinfrastructure.

Source: DHS

INDICATORS OF TERRORIST ATTACKS AGAINST MOTORCADES AND CONVOYS: Motorcades and convoys have been attractive targets of terrorist attacks overseas, but similar attacks in the United States cannot be discounted. Terrorist training manuals and other literature have included information on the proper tactics of such operations. Small-arms ambushes, improvised explosive devices (IEDs), and vehicle-borne improvised explosive devices (VBIEDs) all have been used in attacks on vehicle columns.

Potential Motorcade and Convoy Attack Indicators:

- Interest in or surveillance of all aspects of road travel preparation and execution, to include personnel assigned, travel routes and schedules, detours, and road closures.
- Suspicious persons photographing, videotaping, or monitoring motorcades and convoy routes and operations.
- Suspicious vehicles, to include motorcycles, mopeds, and bicycles loitering near or parked along the route of the motorcade or convoy, proceeding or following the group.
- New, newly placed, or modified mailboxes, trash cans, dumpsters, or vehicles along a motorcade route, which could be used to conceal IEDs.
- Vehicle or bystander concentration at choke points along a motorcade route, such as intersections, underpasses, overpasses, or narrow sections of road with no access in or out.
- Vehicle or bystander concentration on high ground or other positions over watching a motorcade route.

High-Profile Motorcade Attacks:

- In September 2009, at least 16 people were killed, including several Italian soldiers, and 55 were wounded when a suicide VBIED was used to attack a NATO military convoy traveling through a residential area of Kabul, Afghanistan.
- In June 2009, a Russian Government official was gravely wounded when a Chechen suicide bomber rammed his motorcade and detonated a car packed with explosives; at least three people died during the attack.
- In September 2008, militants fired gunshots at the motorcade of Pakistani Prime Minister Yousaf Raza Gillani. The prime minister was not in the motorcade at the time of the shooting. The shots apparently were fired from a hill overlooking the motorcade route.
- In October 2007, over 100 people died and 200 were wounded in a suicide bombing targeting former Pakistani Prime Minister Benazir Bhutto as she was driven in a motorcade through Karachi.
- In December 2003, Pakistani militants linked to both al-Qa'ida and the Taliban made two separate and unsuccessful attempts to assassinate Pakistan President Pervez Musharraf by attacking his motorcades.

Source: DHS/FBI Roll Call Release November 19, 2009

TOXIC INDUSTRIAL CHEMICALS - THE MOST LIKELY TOXIC INDUSTRIAL MATERIALS TO BE USED IN AN ATTACK AGAINST THE UNITED STATES: The FBI assesses domestic or international terrorists would most likely use toxic industrial chemicals (TICs), especially cyanides and chlorine, in any attempted chemical, biological, radiological, or nuclear attack against the United States, owing to the high level of TIC awareness among extremists, the relative ease of acquisition and dissemination of these materials, and the ability to handle TICs safely without advanced training or knowledge. Terrorists are less likely to deploy hazardous radiological material and toxic industrial biologicals because they are more difficult to acquire and handle safely before dissemination.

Source: FBI Current Intelligence Report, 30 October 2009 (UNCLASSIFIED).

TERROR-LINKED ITEM HIDDEN IN BURQA: According to a Transportation Security Administration/Office of Intelligence (TSA/OI) product based on open source reporting, on 2 November 2009 a female UK resident and a Moroccan national who previously lived in Hague, Netherlands—pled guilty in a UK court to charges under the Terrorism Act 2000. She was convicted of possessing an article which gave rise to suspicions that the article was “connected with the commission, preparation, or instigation of an act of terrorism.”

Specifically, on 16 October 2008, the defendant accidentally dropped a memory stick containing “a mini-encyclopedia of weapons-making” from beneath her burqa while she was being questioned at Liverpool John Lennon Airport after arriving on a flight from Amsterdam. The memory stick contained more than 7,000 files, including an explosives manual for “The Brothers of the Mujahedeen.” The device was tied to an inner sleeve of her burqa. A search of defendant’s additional property yielded a handwritten note in which she indicated she and her children would be “bombs for the sake of this religion.” Evidence was also uncovered from Internet chat room sites, in which she indicated her support for those seeking martyrdom.

FBI Newark Comment. Both criminals and terrorists have used burkas to evade law enforcement. In January 2009, a Philadelphia man committed a robbery and violated numerous weapons offenses while wearing a black burka robe and veil. In 2005, one of the perpetrators of the failed 21 July 2005 UK transit bombings fled London wearing a full length black dress and burka.

Source: NCTC Terrorism Summary, 5 November 2009 (UNCLASSIFIED).

CLOROX TO STOP TRANSPORTING CHLORINE IN THE UNITED STATES:

According to a National Capital Regional Intelligence Center (NCRIC) product based on information from the Miami Herald, household products maker The Clorox Company said it is changing how it makes its namesake bleach so it can stop transporting chlorine to US factories by rail amid growing safety concerns and regulatory scrutiny. Starting at its Fairfield, California factory north of San Francisco, Clorox said it plans to switch to high-strength bleach with a higher concentration of sodium hypochlorite instead of buying chlorine and making bleach onsite. Clorox expects to finish the transition in Fairfield within six months.

Comment. A chlorine truck bomb explosion is capable of causing a significant amount of deaths while also injuring others from the inhalation of the toxic fumes. The Iraqi insurgent use of chlorine truck bombs during 2007 prompted the United States to implement new federal regulations on chemical plant security, which includes having Homeland Security teams inspect hundreds of chemical plants that make and store chlorine and other potentially deadly chemicals. The NCRIC does not possess any intelligence indicating that such an attack is imminent or that terrorists have stolen any chlorine from the nation’s chemical or water treatment plants, which use chlorine to purify drinking water.

Source: NCTC Terrorism Summary, 10 November 2009 (UNCLASSIFIED).

RADIO FREQUENCY JAMMERS USED TO DISRUPT COMMUNICATION DEVICES: Radio frequency jammers are devices designed to prevent communication devices from operating by deliberately broadcasting disruptive radio transmissions on the frequencies used by the targeted devices. Radio frequency jammers have been used to interfere with communications between law enforcement officers.

Characteristics of Radio Frequency Jammers

Originally created for law enforcement and the armed forces to interrupt criminal and terrorist communication, radio frequency jammers have been developed for civilian use and are sold illegally on the Internet.

Unlike older radio frequency jammers, which broadcast noise on the target frequency to disrupt communications, newer jammers use more subtle techniques, in which no sound is heard on the targeted equipment.

In October 2008, police in Canada encountered a vehicle driven by supporters of a violent motorcycle gang. The officers noticed that they were unable to transmit radio calls to other officers. During a search of the vehicle, they discovered a radio frequency jammer that blocked their radio transmissions within five meters of the device.



(U) Portable radio frequency jammer hidden in cigarette pack.

Indicators that a radio frequency jammer is in use are:

- Users are unable to transmit on two-way radios.
- Users hear faint music, electronic noises, or other recorded sounds on their designated frequencies.

Portable radio frequency jammers can be concealed in cigarette packs, briefcases, luggage or laptop bags, and can be disguised as a key fob or cell phone car charger. Some jammers are small enough to be plugged into a vehicle cigarette lighter.

This product is intended to assist federal, state, local, and private sector first responders in developing deterrence, prevention, preemption, or response strategies.

LAW ENFORCEMENT INFORMATION NOTICE: This product contains Law Enforcement Sensitive (LES) information. No portion of the LES information should be released to the media, the general public, or over non-secure Internet servers. Release of this information could adversely affect or jeopardize investigative activities.

Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//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 DHS policy relating to FOUO information and is not to be released to the

public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized security personnel without further approval from DHS.

Source: DHS / FBI Roll Call Release, 23 November 2009

FBI ARRESTS FIVE IN OVERSEAS ARMS TRAFFICKING PLOT: The following information is based on initial reporting and is being provided for your situational awareness. If you choose to share this information, in accordance with the handling instructions, you are also required to share any subsequent updates posted by I&A/IWW on this topic.

FBI Arrests Five in Overseas Arms Trafficking Plot

On Saturday, 21 November 2009, the FBI in Philadelphia arrested five men on varying charges that include conspiracy to acquire missile systems designed to destroy aircrafts, transport of stolen property, conspiracy to possess machine guns, conspiracy to commit passport fraud, and conspiracy to transport stolen property.

The individuals reportedly intended to acquire munitions for use by the Resistance, a reference to Palestines conflict with Israel, in the Middle East.

This event appears to be isolated in nature and is not related to any known terrorist plotting against the Homeland. This message is being disseminated for your awareness due to U.S. interests in Israel and the broader Middle East.

IWW anticipates no further reporting on this subject.

ONLINE JIHADISTS EMBRACE FORT HOOD SHOOTINGS: On 5 November 2009, USPER Nidal Malik Hasan opened fire at the Fort Hood military installation, killing 13 people and wounding 29. Although investigators are still determining what factors prompted the attack and whether Hasan indeed acted alone, the incident has become a rallying point for members of jihadist Internet forums and bloggers, including identified extremist Anwar Nassar Al-Awlaki, the former imam of an Islamic center in Northern Virginia frequented by Hasan in 2001. The great majority of postings and comments on these Web sites support the shootings, defend Hasan's actions, and call for others to follow his example.

- Beginning on 5 November 2009, comments on the jihadist Ansar al-Mujahideen forum openly praised the shooter and his actions. Readers of this forum also took the opportunity to reference the 1 June 2009 shooting at a Little Rock, Arkansas, military recruiting station and the recent arrests in Detroit, Michigan of Ummah movement members.
- According to one Web forum participant, “. . . the attack carried the same characteristics as those of al-Qai'da of Jihad [sic], my brothers” and “. . . the only thing you were missing was an explosive belt.”
- Some Internet forum users have displayed their support by adopting Hasan's picture as their avatar and imposing derogatory statements over the images of victims of the shooter.

The viral nature of threads and blogs allow forum users to reach an international audience while retaining a high level of anonymity. Overall, these initial reactions illustrate how seamlessly the Fort Hood shootings have been incorporated into the jihadist narrative of the United States waging a war on Islam.

As comments proliferate anonymously on various jihadist forums, the role of one prominent blogger is emerging as especially significant—that of Anwar al-Awlaki who moved to Yemen in 2004 who yet maintains influence and communication with his followers via his popular English-language blog. Although the extent of their relationship is not yet fully known, Hasan was in communication with the influential US-born imam since 2008.

- On 9 November 2009, al-Awlaki posted a new blog entry titled “Nidal Hassan Did the Right Thing.” The short Web posting labeled Hasan a hero while branding the US War on Terror “a war against Islam.” Ominously, al-Awlaki's posting implicitly argues for other Muslims in the US Army to engage in similar violence, stating “. . . the only way a Muslim could Islamically [sic] justify serving as a soldier in the US Army is if his intention is to follow the footsteps of men like [Hasan].”

While it is unknown whether al-Awlaki was complicit in Hasan's actions, the interaction between Hasan and al-Awlaki indicates the ease with which communication can be established between an identified extremist and his followers. Al-Awlaki's quick response further showcases his ability to capitalize on events irrespective of geography to enhance his standing in the eyes of his readers. These comments—whether anonymous or from leading personalities like al-Awlaki—highlight the growing trend of using social media networks and Internet forums to glorify attacks and rally support for terrorism suspects.

Source: NCRIC Bulletin, 9 November 2009 (UNCLASSIFIED).

X-FLEX BOMB-PROOF WALLPAPER: X-Flex is a new kind of wallpaper: one that's quite possibly stronger than the wall it's on. Invented by Berry Plastics in partnership with the US Army Corps of Engineers, this lifesaving adhesive is designed for use any place that is prone to blasts and other lethal forces, such as in war or natural-disaster zones, chemical plants or airports. To keep a shelter's walls from collapsing in an explosion and to contain all the flying debris, you simply peel off the wallpaper's sticky backing, apply the rollable sheets to the inside of brick or cinder-block walls, and reinforce it with fasteners at the edges. Covering an entire room can take less than an hour. The combination works so well that the Army is now considering wallpapering bases in Iraq and Afghanistan.



Civilians could soon start remodeling too-Berry Plastics plans to develop a commercial version next year.

Source: Florida Intelligence Unit, 25 November 2009 / <http://www.plasticsnet.com/article.mvc/Introducing-X-FLEX-Blast-Protection-System-0001?VNETCOOKIE=NO>

WRTAC Customer Satisfaction Survey

Return to: Washington Regional Threat Analysis Center
 Washington, D.C.
 202-563-2768 (Fax)

Dear Customer,

Please take a moment to complete this survey and help evaluate the quality and value of WRTAC products. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance.

Instructions: Circle the appropriate response according to the following scale.

- 1 Strongly Disagree
- 2 Disagree
- 3 No Opinion
- 4 Agree
- 5 Strongly Agree

N/A Not Applicable

Product Title/Date: _____

Customer: _____

Quality:

1	2	3	4	5	N/A		This product was delivered in a timely manner.
1	2	3	4	5	N/A		This product was relevant to your duties and needs.
1	2	3	4	5	N/A		This product was clear and easy to comprehend.
1	2	3	4	5	N/A		This product resulted in a change in investigative or intelligence priorities.
1	2	3	4	5	N/A		This product resulted in more informed decisions concerning officers' defensive posture and vigilance.
1	2	3	4	5	N/A		This product identified new information on pending matters or offered insights that could change a working premise.