Washington Regional
Threat and Analysis Center
Washington, D.C.
wrtac@dc.gov
202-233-1500
202-233-1427 (Fax)

Washington DC Threat Level

ALERT LEVEL GREEN | ALERT LEVEL BLUE | ALERT LEVEL YELLOW | ALERT LEVEL ORANGE | ALERT LEVEL RED

Alert Level Yellow
ELEVATED CONDITION

Officer Safety & Criminal Intelligence Issues

VOLUME: 2, **ISSUE:** 24 **EFFECTIVE DATE:** 31 December 2008

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

A SURVIVAL TOOL FOR CREATING A TOOL OF SURVIVAL: Originally developed for the Swedish Department of Defence, Swedish FireSteel is a flash of genius. Its nearly 3,000°C spark makes fire building easy in any weather, at any altitude. Used by a number of armies around the world, Swedish FireSteel's dependability has already made it a favourite of survival experts, hunters, fishermen and campers. It has also found its way into cabins and backyards as a fool-proof way to light stoves and gas-barbecues. Amazingly enough it also works equally well when wet. A metal blade is slowly moved across the Firesteel, generating sparks that can easily be thrown onto a small pile of dry grass, leaves or paper to start a fire. When the fire is becoming established, thin sticks of wood can be added, gradually increasing to thicker ones.

Also available: MayaDust - a fire starting material made from Pino de Ocote, a fatwood pine cultivated in the highlands of Guatemala and Mexico. With an 80% resin content, MayaDust is easy to light even when wet and produces an extremely hot flame. Packed in a convenient waterproof tin it gives maximum heat energy for minimal weight. http://www.thinkgeek.com/gadgets/tools/754d/

Source: Peel Regional Police

****

LIFEVEST WEARABLE DEFIBRILLATOR: The LifeVest wearable cardioverter defibrillator is a new treatment option for sudden cardiac arrest that offers patients advanced protection and monitoring as well as improved quality of life.

The LifeVest is the first wearable defibrillator. Unlike an implantable cardioverter defibrillator (ICD), the LifeVest is worn outside the body rather than implanted in the chest. This device continuously monitors the patient's heart with dry, non-adhesive sensing electrodes to detect life-threatening abnormal heart rhythms. If a life-threatening rhythm is detected, the device alerts the patient prior to delivering a shock, and thus allows a conscious patient to disarm the shock. If the patient is unconscious, the device releases a gel over the therapy electrodes and delivers an electrical shock to restore normal rhythm.

Source: www.zoll.lifecor.com

****

RESPONDING TO HYBRID VEHICLE INCIDENTS QUICK REFERENCE GUIDE

General Information

- Most hybrid vehicles look similar to their standard model counterparts.
- Orange cables are used to indicate high-voltage wiring (greater than 60v DC).
- Yellow or Blue cables indicate intermediate-voltage wiring (greater than 30v DC and less than 60v DC)
- High-voltage NiMH batteries are not considered a spill hazard as they are a dry cell battery.
- Immobilize vehicle as soon as possible to prevent unexpected movement.

Standard Disabling Techniques

Option #1

- Remove ignition key and place it on the dashboard. In vehicles equipped with a "Smart Key", move the "key" a minimum of 16 feet from the vehicle.
- Disconnect the 12v battery.

Option #2 (if ignition key is not accessible)

- Disconnect 12v battery.
- Remove high-voltage fuse in engine compartment fuse box.
- Due to the difficulty in trying to remember which fuse controls the high-voltage system in each hybrid make and model, just pull all the fuses in the engine compartment fuse block to ensure that the proper one is removed.
- Additional considerations specific to certain vehicle makes and models can be found on the reverse side.

Hybrid Vehicle Fires

- Use an offensive attack if the NiMH batteries are not involved.
- Use a defensive attack if the NiMH batteries are involved.

Hybrid Model	Battery	Battery Location	Identification	Vehicle Specific Items
Ford Escape/ Mercury Mariner	300v-330v	Rear of vehicle under cargo area carpet	▪ Hybrid logo on lift gate, front driver and passenger doors ▪ Driver's side rear quarter glass has battery vent	▪ Remove high voltage service disconnect switch on the HV battery in the rear cargo area
Honda Accord	144v	Behind rear seat	▪ Hybrid logo on rear of vehicle ▪ Battery vent on rear deck	
Honda Civic	144v	Behind rear seat	▪ Hybrid logo on rear of vehicle ▪ Battery vent on rear deck	
Honda Insight	144v	Under rear cargo area	▪ Unique aerodynamic shape ▪ Insight and hybrid logo on rear of vehicle	
Toyota Prius 1st Generation (2001-03)	274v	Behind rear seat	▪ Hybrid logo on trunk ▪ Battery vent on the driver's side C-pillar	
Toyota Prius 2nd Generation (2004-)	201v	Behind rear seat	▪ Hybrid Synergy Drive logo on rear hatchback door	▪ If equipped, use the disable "Smart Key" button under the steering column ▪ Keep "Smart Key" 16 feet from vehicle
Toyota Highlander	288v	Under second row seat	▪ Hybrid Synergy Drive logo on the lift gate	
Toyota Camry	245v	Behind rear seat	▪ Hybrid logo on trunk , driver and passenger front fenders ▪ Battery vent on rear deck	▪ Keep "Smart Key" 16 feet from vehicle
Lexus RX 400h	288v	Under second row seat	▪ Lexus RX 400h on the lift gate	
Lexus GS 450h	288v	Behind rear seat	▪ GS 450h logo on trunk and hybrid logo on the rear doors	▪ Keep "Smart Key" 16 feet from vehicle
Nissan Altima	245v	Behind rear seat	▪ Hybrid logo on front doors and trunk ▪ Battery vent on rear deck	▪ 12v battery is located in the trunk ▪ NiMH battery service disconnect in the trunk ▪ Keep "Intelligent Key" 16 feet from vehicle
Chevy Silverado/ GMC Sierra	42v	Under rear seat	▪ Hybrid logo on the doors and dashboard	▪ Manual disconnect on passenger side of the battery storage area under rear seat ▪ Uses lead-acid batteries
Saturn VUE	36v	Behind rear seat under cargo area	▪ Hybrid logo on front doors and rear hatchback	▪ Blue cable for 36v hybrid electrical system ▪ NiMH battery service disconnect under access plate

Source: Emergency Training Solutions, 1-800-485-1161

DOOR SHANKS: A product called **"Doorshanks"** is being sold on-line and is marketed as a tool to allow "law abiding" citizens a method to gain entry into their car (lost keys, keys locked in car, etc.). The website: www.doorshanks.com notes that the tool will allow entry into a car in under 6 seconds and the inventor is a "former" professional car thief.

The doorshank is inserted in the lock and turned with a socket/wrench to force open the locking mechanism. Instructions along with video links are posted on the website.

Source: MTA – NY Police Department, Daily Intelligence Briefing, 17 December 2008

****

GUN KNIFE: On 17 December 2008, a Town of Warwick Police Officer recovered the below imitation pistol/knife from a vehicle during a traffic stop. Pulling the hammer activates the knife. Suspect would not give information on how he obtained the below weapon.

Source: Warwick Department of Police, New York

TOTER'S JEANS: This is a legitimate company marketing jeans in the Southern USA and producing them with built-in gun and knife pockets. The gun pockets are lined and can be bought for both left or right hand carry. The pockets are lined with non-abrasive Cordura-Plus and are designed to conceal the silhouette of the gun. The gun pockets have a patent pending lacing system that is adjustable to fit most handguns. Toter's also produces jackets, vests and T-shirts that guarantee total concealment.

Source: MTA – NY Police Department, Daily Intelligence Briefing 29 December 2008

****

HAIRBRUSH DAGGER: It looks like an ordinary hairbrush, but the handle is actually a highly effective dagger knife! The blade cross-section is cruciform in shape and a full 1/2" thick. It tapers gradually along its 3 1/2" length down to a needle-like point. And like any good dagger (or hairbrush) it has a well-designed secure handgrip. The Honey Comb is precision injection molded from Zytel® a super tough nylon and fiberglass composite that contains no metal and is impervious to the elements. With its innocent appearance and obvious usefulness (after all it is a real hairbrush), this is the answer to personal defense at home at work or overseas. As a hairbrush it's particularly appropriate when carried in a glove compartment, travel luggage, or a woman's handbag and will look perfectly natural in virtually every room in your house.

Weight: 2.2 oz.
Overall: 7 7/8" w/o brush
8 1/4" w/ brush

For additional information refer to the following link: http://www.defensedevices.com/brush-knife.html

Source: MTA – NY Police Department, Daily Intelligence Briefing 25 December 2008

CAR-USE GPS JAMMER: The pictured unit, a GMC07, is a tiny device that blocks GPS tracking and data logging units. It could disrupt GPS logging/tracking/navigation systems, which may work on your vehicle or a suspect vehicle involved in an investigation. Most undercover devices can be quickly installed on a car/truck and allow users to track the movements of a vehicle. This GMC07 will disable the GPS link and render the undercover device useless.

Source: Delaware Information & Analysis Center Daily Roll-Call Bulletin 29 December 2008

****

CONCEALMENT PANTS: The Tactical Concealment Pant is built to offer lasting performance, comfort, and to meets all concealment needs. No need to buy a holster...it's included in these pants.

Includes a holster made from surgical grade elastic that is already sewn into the pants which holds your gun securely! The pants also have a second all-purpose concealment pocket to store a spare magazine, cellphone, iPod, passport, wallet or other small valuables.

For additional information refer to the following link: http://masterofconcealment.com/pgroup_descrip/106_Concealment+Items/7097_Tactical+Concealment+Pant/?mode=image&image=258

Comment: L/E should be reminded that these products are primarily sold to law enforcement personnel but are available for sale to all. The hidden pocket can be used to conceal many items that pose a threat to law enforcement officials. When a subject is rear cuffed, a preliminary check of the subject's waist line should be preformed to detect any possible threats.

Source: MTA – NY Police Department, Daily Intelligence Briefing 30 December 2008

****

THE WORLDS MOST POWERFUL HANDGUN: The world's most powerful pistol is the Austrian Pfeifer-Zeliska .600 Nitro Express Magnum. It is chambered to fire the British developed .600 caliber rifle bullet originally made by Holland and Holland. This revolver was not originally a full production model but a one off built especially for a wealthy Swiss gent...Mr. Zeliska. Bu t if you would like one and I am sure that a few of you licensed rootin tootin gun lovers with a bit of disposable income would, then contact Pfeifer arms (url near bottom of page) and they will make one for you. Priced at 13,840 Euro's. This equates as $16,501 or £9,417 (Exchange rate Feb 24th 2006) The Pfeifer Revolver is also available chambered for the .458 Winchester Magnum and qualifies as the second worlds most powerful handgun.

The .600 Nitro Express bullet was originally developed in 1899 for the big game hunters who went to Africa with the intention of killing Elephants. Even though H&H no longer manufacture these cartridges they can still be sought through the gun trade, small reloading companies or even over the internet.

One company still actually makes these rounds and they are Kynoch at www.kynochusa.com

Of course the size of cartridge based ammunition can go up to an 88mm anti-tank round and beyond but as small arms go, these bullets/cartridges are colossal. Nitro Express in firearms terms applies to a cartridges charge or powder that in this instance is made by mixing nitroglycerine with the already explosive gunpowder to make a nitrocellulose compound which is then dried and becomes many times more explosive than the original gunpowder. With a Bullet Weight of 900 grains and a Muzzle Velocity 1950 fps, it produces Muzzle Energy of 7591 ft/lbs or 3½ tons!! the Pfeifer- Zeliska .600 Nitro Express Magnum is 8 times more powerful than a

Smith and Wess on.44 magnum and 3 times more powerful than the Smith and Wesson .50 Magnum. The 'Mag-Port' recoil compensation holes can be seen at the business end of the barrel, these holes let some of the blast out before the bullet has left the barrel, in so reducing the back pressure enough to lower the recoil to an acceptable degree. In fact the gun 'only' rises up 60 degrees when fired. The line of sight from rear to front sight is 440mm. This long sight range of course helps for long range shooting of which the .600 is more than capable.

For additional information refer to the following links:

http://www.vincelewis.net/50magnum/600-gun-3.JPG

http://www.vincelewis.net/50magnum/600_Nitro_Express.jpg

Source: MTA – NY Police Department, Daily Intelligence Briefing 30 December 2008

****

DISGUISED ITEM: The Q-FOB is a new product built to imitate the look and design of an electronic vehicle key. However, the Q-FOB is a key camera which includes features such as a USB rechargeable battery, built-in time stamp, 90 minutes of video recording time and two GB of memory.

SPECIFICATIONS:
Resolutions: 3.1 megapixels Time Stamp: Date, Hour
Image Sensor: 1/3” Memory Capacity: 2GB
Compression (Photo): JPEG, Capacity: Over 1,600 Images; PC Interface: USB 2.0
Compression (Video): MPEG4 AVI Recording capacity: 2.86hrs
Compression (Audio): AMR: 16 hrs Indicators: Vibrations, LED
Internal Battery: Li-Polymer (90 mins) Rechargeable via USB Size: 28mm x 70mm x 16mm
Weight: 18g Price: $42.00-$87.99

Source: Indiana Intelligence Fusion Center

CRIMINAL INTELLIGENCE

DATA SHOWS JUVENILES INVOLVED IN MANY DOMESTIC EXPLOSIVE INCIDENTS: The latest data available on domestic explosive incidents shows that juveniles are involved in more of these 2,700 incidents than any other group. "Six out of 10 of these explosive incidents involve juveniles," said Scott Sweetow, the assistant special agent in charge of Atlanta's field office for the Bureau of Alcohol, Tobacco, Firearms and Explosives. "It's shocking and, in fact, it's not well known," Sweetow said. "And, it's not something that's going to go away." The latest figures, gathered by the ATF reveal that between 2004 and 2007 juveniles accounted for well more than half of all reported traceable explosive incidents - far exceeding gangs and hate groups combined. This year alone, news reports cite at least 106 arrests nationwide of teenage boys for either manufacturing bombs or plotting to set them off.

- In Arizona, eight students were hospitalized after a teen detonated a bomb at his school.
- In North Carolina, a 13-year-old boy made a bomb that burned the face of a 7-year-old girl.
- In Kansas, a teen bombing destroyed part of an apartment building.

The key components of high-powered bombs are readily available at your local hardware store, with no federal law preventing minors from buying most of the ingredients. Detailed instructions on how to create military-style explosives are all over the Internet, too.

Source: Wisconsin Statewide Information Center – Daily Intelligence Briefing, 15 December 2008

****

TROOPER STOPS MOBILE ID LAB IN TENNESSEE: A Tennessee State Trooper recently observed a Ford Escort visibly advertising identification cards that could be made in ten minutes. The vehicle did not have a commercial license plate (H-1 tag) required for vehicles used in a commercial enterprise. Upon stopping the driver for the violation, the Trooper observed a portable computer in the front seat and a card printer for producing plastic IDs in the rear seat. After obtaining consent to search the vehicle, Troopers recovered several fake Tennessee and Florida ID's. The driver was taken into custody and booked on charges of manufacturing government documents, suspended drivers license, possession of more than one

driver's license, and registration law (furtherance of a business not displaying a commercial tag). Agents are conducting an ongoing investigation into the fraudulent identification cards and possible federal violations. The ID cards were very close to authentic and might easily fool a financial or business operation.

Source: Virginia Fusion Center

****

METHAMPHETAMINE CAPSULES: In October 2008 the Statewide Terrorism and Intelligence Center (STIC) received information officers in Jackson County, Missouri, recovered a number of methamphetamine capsules stored inside prescription pill bottles. Officers discovered the prescription medication had been taken out of the gel caps and replaced with methamphetamine as shown below. Numerous addicts and recovering addicts stated the altered capsules were popular among users while in the work place because the concealment offered a discreet way to get high. A search of Drug Enforcement (DEA) and El Paso Intelligence Center (EPIC) records was negative on this swap-meds-with-meth method. An open source search revealed a chat room discussion where questions were posed regarding the use of "meth capsules."

Analyst Comment: In 2005, Illinois State Police (ISP) agents with the Quad City Metropolitan Enforcement Group (QCMEG) seized $15,350 United States Currency (USC) from a vehicle subsequent to an I-80 traffic stop. A K9 alerted on the vehicle, and a search revealed a

prescription bottle with a small number of gel capsules which tested positive for methamphetamine. Law enforcement officers should be cognizant of this method of concealing meth.

Source: Jackson County Drug Task Force, STIC Intelligence Files

****

GANGS INFILTRATE AIRPORTS: Organized gangs and smugglers are infiltrating Canada's biggest airports, providing a breeding ground for international terrorism, critics say, citing information from a recently revealed federal police investigation. A two-year probe by the Royal Canadian Mounted Police (RCMP), the country's national policing agency, shows that 58 organized gangs are smuggling drugs into the country's airports, including Toronto, Montreal, and Vancouver. Many of the gang members are airport employees, including baggage handlers and customs agents, who have used their security clearances to thwart the law.

The insider, who holds a position of trust with access, represents one of the greatest threats to aviation because he/she is extremely difficult to counter. In the past, insider access has been utilized almost exclusively to smuggle illicit goods, drugs and weapons, as well as humans, although this access has also been used to attack aviation.

- The most notorious terrorist incident using insider support was the bombing of Pan Am Flight 103 in December 1988. Libyan intelligence agent Ali al-Megrahi, working undercover as the station manager for Libyan Arab Airlines, aided in the placement of a suitcase bomb aboard an Air Malta flight at Luqa Airport in Malta. That suitcase was eventually transferred onto Pan Am Flight 103 bound for New York. The device detonated as the aircraft flew over Lockerbie, Scotland, killing all 259 people onboard and 11 people on the ground.

Terrorists have also been able to bribe insiders to carry out attacks. Investigators have proven repeatedly that insiders can be bribed, cajoled, or extorted into placing just about anything onto an aircraft.
Terrorist organizations have expressed interest in recruiting specific individuals based on their positions, skills, levels of access to critical areas, or physical/cultural characteristics. Western converts or radicalized Westerners are of particular interest.

Analyst Comment: A presence of organized crime indicates a susceptibility to acts of terrorism.

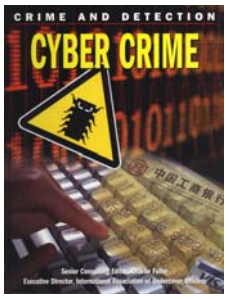
Source: TSA-OI Civil Aviation Assessment 2007-2008 / http://www.csmonitor.com/2008/1216/p06s01-wogn.html

****

Monikers Resurfaces as Possible Intimidation Tactic by Animal Rights Extremists: Animal Rights (AR) extremists using the monikers Animal Rights Militia (ARM) and Justice Department (JD) claimed responsibility in November 2008 for separate acts of vandalism in California against university researchers and threatened continued attacks. ARM and JD are not groups but rather monikers under which AR extremists claim actions. The FBI assess in the two recent incidents the names likely were adopted to intimidate victims, recalling past violence actions committed under the auspices of ARM and JD. A communiqué dated 9 November 2008 claimed ARM was responsible for vandalizing the home of a University of California (UC)-Berkeley researcher. A communiqué dated 13 November 2008 claimed responsibility under auspices of JD for vandalism at a UC-San Francisco researcher's home. Both communiqués threatened further attacks against researchers. The ARM name has been cited in claims of responsibility for violent acts in Europe and North American since the 1980s – including hoax poisonings, improvised incendiary devices, letter bombs, threatening letters, and grave desecration – some of which have since been attributed to specific individuals or groups. The JD moniker appeared in claims of responsibility throughout the 1990s in the United Kingdom for a string of letter bombs, some of which caused serious injuries to recipients, and in North America in connection with a string of threatening letters, some of which contained razor blades coated with rat poison.

Source: FBIHQ – Counterterrorism Analysis Section via FBI Weekly Intelligence Report

****



CYBER CRIMINALS BECOMING MORE ORGANIZED: The common view of computer hackers as lone attackers is no longer accurate. Security researchers increasingly are seeing cyber criminals use tactics that hint at a higher degree of organization and sophistication, creating a new breed of hacker that is more efficient and more capable. Cyber crime has evolved into a large shadow economy organized much like the legitimate business world, according to a report by a cyber security firm. Cyber criminals have developed a system of easily executed and sophisticated attacks that allow them to focus on managing the data they steal while remaining undetected.

- The new cyber crime model mirrors legitimate business models: supplying a customer with a product or service and generating revenue. The "for-profit" approach is a shift in the realm of cyber crime from the "hack for fame" model.

Cyber criminal groups have developed into modern hierarchical organizations with reward systems in which each criminal has a well-defined role. Many experts have pointed out that these organizations' structures strongly resemble those of traditional organized crime groups, which also took their operating principles from corporations.

- Both cyber criminals and some organized crime groups have a "boss" at the top of the organization who operates as a business entrepreneur or business manager, while subordinates commit the criminal activity.

- "Campaign managers," like Mafia capos, lead attacks using software such as the Trojan Command and Control to manage these campaigns remotely. The malicious code invades the machines of unsuspecting visitors to legitimate sites, collecting data from infected machines. The attackers' toolkits contain sophisticated antiforensic techniques that complicate tracing and detection.

- Similar to Mafia "associates," "stolen data resellers" are crucial to a cyber crime organization. They are not involved in attacks but resell the collected data.

- The "affiliation networks" of hackers spread malicious code references to legitimate websites. A cyber security firm reports that it has identified six active affiliation networks or programs that exist on hundreds of legitimate websites. The hackers are paid by the amount of successful infections they produce. As in any business, tracking and management tools have been emerging on crimeware servers.

Any organization with a website is vulnerable to these sophisticated and swift attacks. The damage to the organization and its loss of data can be extensive. For protection, security firms recommend a layered security approach, as well as new tools such as real-time code inspection technology to prevent, detect, and manage the threat. Real-time code inspection technology detects malicious code directly without using signature updates, databases, or classified uniform resource locators. Analyzing content regardless of its origin, such technology will detect malicious code and prevent it from reaching the corporate network, even if the code originates from a trusted but infected site.

Source: DHS Cyber Security – Volume 1, Number 11

IDENTIFICATION OF A METHOD USED TO TRAFFIC UNTAXED CIGARETTE PROCEEDS FROM NEW YORK TO JORDAN, AS OF JULY 2008: As of July 2008, unidentified individuals paid Jordanian military security officers, assigned as law enforcement officers to Royal Jordanian Airlines USD 300 to carry USD 50,000 of untaxed proceeds through security checkpoints at John F. Kennedy International Airport in New York and on into Jordan. Individuals involved in New York approached military officers at their hotel. (Source comment: Jordanian military officers always stay in the same hotel rooms at an identified US hotel in New York.) In late April 2008, an identified USPER was convicted of third degree money laundering when he/she attempted to traffic untaxed cigarette proceeds to Jordan. The airline used was Jordanian Airlines. The airline is the conveyance that the military officers are using to transport the money. The ultimate recipient of the proceeds remain unknown. Untaxed cigarette proceeds are illegally obtained, unknown to law enforcement or controlled substance regulatory authorities, and sold at full price. The proceeds of the sell are pocketed instead of forwarded to the tax authority.

Source: FBI IIR 4 214 1530 09

****

PLANNED ORGANIZATION OF A NEW ARMED UNIT WITHIN THE NATIONAL SOCIALIST MOVEMENT, AS OF SEPTEMBER 2008: As of September 2008, the New York unit of the National Socialist Movement planned to organize and train a new armed unit within the National Socialist Movement that was to be tasked with protecting the national socialist movement commander and other personnel.

Source A provided the information in paragraph three.

As of August 2008, the National Socialist Movement (NSM) planned to organize and train a new armed unit within the NSM that was to be tasked with the duty of protecting the identified NSM commander and other unidentified NSM personnel. The NSM intended for members of the new armed unit to be trained in New York, to learn proper firearms skills, and to legally obtain a Federal HR-218 Permit to Carry a Firearms Interstate. (FBI comment: The Federal HR-218 permit, issued to active and retired law enforcement officers, allows licensees to carry concealed firearms in any jurisdiction within the United States, regardless of state and local laws to the contrary.)

Source B provided the information in paragraph five.

As of September 2008, the NSM planned to organize and train a new armed unit of the NSM, tasked with the duty of protecting the identified NSM commander and other unidentified NMS personnel. As of September 2008, the NSM planned to recruit members who lacked a criminal record or who could legally obtain a permit to carry a concealed handgun. The NSM intended to train members of the new armed unit in the use of rifles, shotguns, and handguns at an unspecified location in New York (NFI).

The National Socialist Movement (NSM) is the largest neo-Nazi group in the United States, known for openly promoting an anti Semitic and racist ideology and an anti-immigration avocation. The NSM, headquartered in Detroit, Michigan, has stockpiled weapons and ammunition in anticipation of waging war against blacks, Jews, Hispanics, and the Federal Government. NSM members have engaged in the procurement of firearms, the alteration of weapons to full automatic capabilities, and paramilitary training, including weapons, combat tactics, and small team tactics training.

Source: FBI IIR 4 201 1943 09

****

CONCEALMENT METHOD: During a recent search conducted at the Wicomico County, Maryland Detention Center, two cell phones and other contraband were found inside inmates tennis shoes. As you can see in the following pictures, the tennis shoes are of the same brand and model (NIKE AIR). The insoles of the shoes were removed and the interior of the sole was precisely cut to make a square compartment that easily hides a cell phone, a cell phone charger or any other contraband. These tennis shoes were sent to WCDC via postal mail from Baltimore; they were purchased at two different shoe stores and were mailed in by these stores. We believe that these shoes a initially bought, the soles are cut, the contraband introduced, then resealed and taken back to the store probably claiming that “The detention center wont accept them unless they are coming directly from the store”.


NIKE
AIR


Johnnie Buttler
96042565
Johnnie Buttler

Source: Maryland Department of Corrections – Intelligence Unit, Wicomico County, MD

****

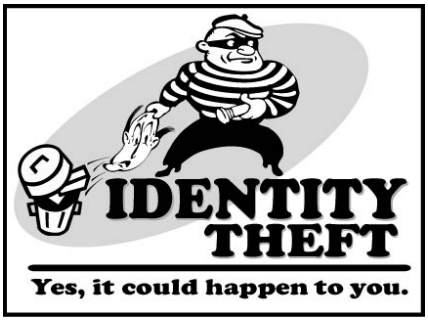
HIDDEN POCKETS IN JEANS: Some jeans can have hidden pockets in the seam. When closed, these pockets can be almost invisible. The pockets can be secured with Velcro, appearing unaltered. In some cases these pockets are large enough to hold threat items such as pocket knives.

Source: Canadian Air Transport Security Authority Bulletin via the Metropolitan Transportation Authority Police Department – New York, 24 December, 2008

ECSTASY MIMIC TABLETS IN PORTLAND, OREGON: The Portland Metro Forensic Laboratory of the Oregon State Police recently received 18 vibrantly colored tablets of five different types, all suspected Ecstasy (see Photos 5 and 6). The exhibits were seized in Portland by the Portland Police Department, incidental to a stop for a traffic violation and subsequent consent search. The tablets were mixed together; there were six round orange tablets imprinted with an Interstate 5 shield logo (total net mass 1.7 grams), four green tablets, shaped and imprinted to resemble a "Transformer"(total net mass 1.1 grams), four round purple tablets imprinted with an JL Audio logo (total net mass 1.2 grams), three pink tablets, shaped and imprinted to resemble the head of Bart Simpson (total net mass 0.8 grams), and one round blue tablet imprinted with the Superman logo (total net mass 0.2 grams). The Transformer and Bart Simpson tablets were very detailed and well pressed, and more resembled candies or children's chewable vitamins as opposed to typical Ecstasy tablets. Analysis by color tests (Marquis and nitroprusside), GC/MS, and UV, however, indicated not MDMA but rather a 1:1 mixture of benzylpiperazine (BZP) and trifluoromethylphenylpiperazine (TFMPP) for the orange, green, purple and blue tablets, and a 1:2 mixture of BZP and TFMPP for the pink tablets. The piperazines were not formally quantitated, but were present in a moderate to high loading based on the TIC and UV. The laboratory has received numerous Ecstasy mimic tablets containing this piperazine mixture over the past year, but never before in these unusual tablet shapes. Since this initial submission, the laboratory received an exhibit containing another 30 of the green Transformer-shaped and imprinted tablets, also containing the 1:1 mixture of BZP and TFMPP.

WRTAC Analyst Comment: The above tablets resemble children's vitamins or candy and could be very attractive to a child because of the bright colors. A child could ingest one or more of these tablets placing the child in a life threatening overdose situation.

Source: Drug Enforcement Administration Microgram



TARGETING OF PRISONERS FOR IDENTITY THEFT: A SPECULATIVE ANALYSIS: Information recently received by the FBI raises the possibility that perpetrators of identity theft may be targeting prison inmates, in the belief that such theft will go undetected for extended periods of time. This is the first reported instance of an inmate becoming a victim of identity theft; however, prisoners likely have great difficulty monitoring their credit than non-incarcerated individuals, which might prevent detection and reporting of such identity theft. If so, other prisoners may be victims of identity theft.

Case Information

A Pennsylvania inmate recently requested the FBI to investigate the theft of his identity. According to this victim, previous to 2005, he had not established a line of credit but at that time, he applied for and was denied credit due to delinquent debts listed on a credit history in his name. The victim requested his credit reports, which revealed that his identity was fraudulently used to open lines of credit since 1996, just three months after his initial arrest and incarceration. Between 1998 and 2004, four of the fraudulent credit lines were subjected to civil judgments for non-payment, and three others were closed by creditors as bad debts. Apparently, the perpetrator who stole his identity pleaded guilty to the four judgments, which, along with the bad debts, were added to the victim's credit report. The as yet unidentified perpetrator also used the victim's personal information to obtain a Massachusetts driver's license. It is unknown how the victim's identity was stolen.

Reasons for Targeting Prisoners

Perpetrators may find targeting prisoners attractive because the stolen identity can be maintained for an extended period of time. The perpetrator(s) in this case apparently used the victim's identity for nearly ten years before the theft was discovered. Because the theft went undiscovered for so long, the perpetrator(s) may have been encouraged to steal or help others steal additional prisoner identities.

Because of limited or varying levels of Internet and telephone access, prisoners with no credit history before incarceration might be unable to open new lines of credit or check their credit status while in prison. Those with credit histories before incarceration may have limited means of monitoring their credit status from prison. In addition, if a perpetrator committed crimes using the victim's identity, the incarcerated victim would likely have no knowledge of the crimes and could not appeal them.

Means of Stealing Prisoners' Identities

The FBI has not yet determined how the Pennsylvania inmate's identity was stolen. The public availability of many arrest and prison records could provide a perpetrator an easy way to identify potential victim's line. Typical cyber identity theft techniques include using deceptive e-mail or Web sites, which, when opened or visited, allow perpetrators surreptitious access to victims' identifying information. Deceptive Web sites with particular appeal to prisoners might include online dating and pen pal sites or unsolicited offers of legal representation. Identity information could be accessed via an undiscovered or unreported data loss or theft from a court or prison computer system or from other records. Identity theft may occur through dumpster diving, or social engineering or the victim or of court or prison personnel with access to inmates' data.

Alternative theories exist that could indicate that perpetrators are not targeting prisoners for identity theft. For example, the above victim was not incarcerated continuously. If his identity was stolen during a period he was out on parole, then he likely was not targeted due to his previous incarceration. Another possibility, which would constitute fraud not identity theft, is that the prisoner victim sold or gave away his identification information. In a separate FBI investigation, prisoners facing long sentences sold their identification information to a fellow inmate who used it for fraudulent purposes. According to US Bureau of Prisons' officials with direct access to the information, USPER Dale Jacobi, while incarcerated, induced Mexican inmates to file fraudulent incorporation documents in their names. Jacobi, working with a non-inmate used the identification information to establish a fictitious law firm and obtain lines of credit.

The hypothesis that perpetrators may be stealing the identification information of inmates warrants discussion and monitoring because, if accurate, a broader pattern of unreported and undetected crimes may be indicated.

Source: FBI - Domestic Thefts and Technology Cyber Intelligence Unit Bulletin – Directorate of Intelligence

****

HEROIN AND COCAINE CONCEALED IN GUITARS: On November 23, 2008, at the Buenos Aires International Airport (EZE) in Buenos Aires, Argentina, officers arrested a commercial air passenger who was attempting to board American Airlines flight 956, a direct flight from Buenos Aires to JFK Airport in New York. An inspection of the passenger's luggage resulted in the seizure of 3.1 kilograms of heroin, consisting of five custom-sized pieces that were secreted within the hollowed-out frame of a wooden electric guitar. *(Source: DEA AMEMBASSY Buenos Aires.)*



On May 5, 2008, Asunción newspaper *La Nación*, reported that Paraguay's National Counternarcotics Secretariat (SENAD) arrested a well-known member of the National Republican Association – Colorado Party politician and his two alleged accomplices, for attempting to send 6.8 kilograms of high-purity cocaine to Europe inside two guitars and a harp onboard a flight from Asunción, Paraguay. (*Source: Southern Cone Crime and Narcotis Issues May 5, 2008, Asunción La Nacion in Spanish – Independent Daily, www.opensource.)*

On February 2, 2008, the Panamanian National Police reported the seizure of 1.5 kilograms of cocaine concealed inside the console of an electric guitar at a security checkpoint at the Tocumen International Airport in Panama City, Panama. The cocaine was wrapped with carbon paper and tape. The Panamanian police arrested two Costa Rican nationals, ages 25 and 42, in connection with this incident. The subjects were boarding a flight to Peru, with connections to Amsterdam, The Netherlands, and Zurich, Switzerland, probable destinations of the drug. *(Source: Multiple source reporting).*

On October 25, 2007, an Italian tourist arriving from Costa Rica and holding tight to his guitar caught the attention of the Guardia di Finanza [Italian Police Force Financial Guard] at the Rome Airport Fiumicino in Rome, Italy. The passenger, a native from Perugia, Italy, was arrested after Guardia di Finanza police officers found cocaine hidden inside the instrument as well as liquid cocaine in thermos-type plastic glasses. Over 3 kilograms of pure cocaine were recovered. *(Source: Joint Interagency Task Force South, International Narcoterrorism Weekly Round-Up, 10/26/07-11/02/07, RWB 2007- Volume XXXV; Roma, La Republica 25OCT07.)*

Source: El Paso Intelligence Center – Domestic Drug Movement Team Bulletin EB08-97

****

CBP SEIZES TEA BAGS FILLED WITH MARIJUANA; ARRESTS TRAVELER
Sterling, Va. – Some people enjoy consuming tea for its antioxidant health benefits while others enjoy tea for the caffeine rush, but for one international traveler, his tea was more the mind altering kind. Unfortunately for him, it couldn't alter an outstanding New York City arrest charge that abruptly ended his return trip home late Wednesday night. Jeffrey Cannon, 20, of Huntington, Md., was arrested by Metropolitan Washington Airports Authority (MWAA) Police after Customs and Border Protection officers confirmed Cannon's identity and his New York City arrest warrant on a DUI charge.

"CBP employees take tremendous pride in our critical role of protecting the nation at our ports of entry," said Christopher Hess, CBP Port Director for the Port of Washington. "It is important for our national security that CBP has advanced information for persons arriving at US air ports of entry. Fugitives from justice should be warned." Cannon arrived to Dulles International Airport at about 3:30 p.m. on Wednesday aboard an Aer Lingus flight from Dublin, Ireland. While confirming Cannon's identify, Customs and Border Protection officers discovered an elaborate smoking pipe with dark residue, an opened bottle of absinthe and a large amount of tea bags. Four tea bags were noticeably larger than the others. Two tea bags contained a green leafy substance; the two others contained a dark brown substance. A CBP narcotics canine alerted to the tea bags and field tests proved positive for marijuana and hashish. CBP officers seized 3.7 grams of hashish, 2.3 grams of marijuana, the smoking pipe and the absinthe and released Cannon to MWAA officers at about 9:30 p.m. "Regardless of the quantity, we have zero tolerance when it comes to illicit narcotics," said Christopher Hess, CBP Port Director for the Port of Washington. "Travelers need to know that if something is illegal in the United States then they should think twice about attempting to bring it here. Our officers and agriculture specialists are trained and highly skilled at detecting prohibited items." International travelers should be aware of the rules for bringing items into the country. CBP consolidates travel information on its Travel Web site.

Source: U.S. Customs and Border Protection

****

TECHNIQUE TO MODIFY AND UTILIZE A UNIVERSAL SERIAL BUS (USB) FLASH DRIVE AS A HIDDEN MASS STORAGE DEVICE: The FBI recently discovered a published set of instructions that described how to modify a Universal Serial Bus (USB) flash device in order to use it as a concealed mass storage device. The article instructed readers how to custom wire a USB flash drive inside a standard telephone wall jack. Subsequently, the USB flash drive was connected to a telephone (RJ-11) cable that was modified to connect to a personal computer using a USB connector. The concept used in modifying a USB thumb drive could be modified to work with any external storage media device that is powered by a USB cable. The finished product allowed the user to store electronic data on the USB flash drive

hidden in the wall of the residence. To the casual observer, the mass storage device appeared to be a normal telephone outlet. A storage device disguised as a standard telephone outlet could be easily overlooked during the execution of a search warrant. This technique could be utilized by any individual that desired a method to covertly store data in a location that is not in the same physical space as their computer. This concealment method could be utilized by child pornographers to secure their collections or other criminals attempting to hide financial records or other incriminating data.

Source: FBI – San Antonio Field Office, Situational Intelligence Report

****

CONTRABAND HIDDEN IN TV CONVERTER: On 12/16/2008, investigators at the Lebanon Correctional Institution intercepted contraband secreted in the interior of a Digital- to -Analog converter box. The contraband was placed in the interior of a MAGNAVOX TB100MG6 Digital to Analog Converter that was shipped to an inmate at the facility. This is the first occurrence of using the converter boxes in the Ohio Correctional System to smuggle contraband.

Comment: Federal law mandates that February 17, 2009 is the last day of full-power analog television broadcasting. Government agencies, industry, public interest groups, and other interested organizations have been working to make sure that the deadline is met and that everyone is prepared for the end of full-power analog television broadcasting. As a result it is anticipated that future attempts will be made using similar equipment, since the inmate television service in their cells is currently limited to analog reception only.

Source: Ohio State Highway Patrol – Office of Investigative Services: Criminal Intelligence Unit Bulletin # 2008-1162

ITEMS of INTEREST

U.S. COCAINE MARKET DISRUPTED - PRICES CONTINUE 21-MONTH SURGE The prices of cocaine and methamphetamine in the United States have risen significantly over the past 21 months, while purity of the drugs has decreased, according to continued analysis of cocaine and methamphetamine seizures by the Drug Enforcement Administration (DEA). From January 2007 to September 2008, the price per pure gram of c ocaine increased 89 percent, from $96.61 to $182.73, while purity decreased 32.1 percent, from 67 to 46 percent. During the same timeframe, the price per pure gram of methamphetamine increased over 23 percent, from $148.91 to $184.09, while the purity decreased 8.3 percent, from 57 percent to 52 percent. “For almost two years the illicit drug market has been showing signs of distress,” said DEA Acting Administrator. “These price and purity trends are not just an immediate reaction from a single enforcement operation, but the result of continuous and persistent progress DEA is making in concert with our international and domestic partners. Across the United States, Mexico, and Colombia and the transit zones in between, we are crippling the world’s leading drug networks, and these prolonged trends confirm that we have disrupted the illicit drug supply chain and U.S. market for cocaine and meth.” These positive numbers illustrate the effectiveness of DEA’s collaborative efforts with Mexico and Colombia, working hand in hand to cripple drug cartels by depriving them of their profits. Since assuming office two years ago in Mexico, President Calderon has taken on corruption and drug trafficking at every level, and has ordered the extradition of unprecedented numbers of drug criminals to the United States from each of the four major cartels. Simultaneously, Colombian President has taken on the FARC and AUC at unprecedented levels, expelling AUC leaders and taking the fight to the FARC. Colombia continues to remain the number one extradition partner of the United States and Mexico is extraditing drug criminals in record rates. "These successes illustrate the unprecedented cooperation we enjoy with Mexico and the United States in battling against international drug trafficking and violence. We cannot battle these sophisticated drug organizations without the collaborative efforts of Colombian, Mexican and U.S. law enforcement and the sharing of information and resources. As a result of this increased success, we have seen more seizures, more arrests, and more extraditions of drug criminals than ever before,” said Colombia Vice Minister of Defense. "The Mexican government has emphasized the significance of downgrading the drug traffickers' ability to generate income by targeting not only their command and control structure, but additionally their logistics for smuggling drugs, cash and weaponry,” said Mexican Attorney General. “With less money available to corrupt or intimidate authorities and their communities, drug traffickers will eventually revert back into a

law enforcement problem, dealt with by regular police forces as opposed to being the threat they currently are to Mexico's national security. Mexico is committed to this struggle, and maintains a mutually beneficial cooperation with law enforcement institutions from other nations -- particularly in the U.S. -- to combat drug traffickers' activities with the ultimate goal of eradicating their pernicious and illegal trade."

DEA/Mexico/Colombia Recent Successes

The continued analysis highlights the momentum created by the efforts among DEA, its U.S. law enforcement partners, Mexico, and Colombia. Just recently, DEA and Mexican law enforcement worked together to arrest Eduardo Arellano-Felix, one of Mexico's biggest drug trafficking criminals and a leader of the Tijuana Cartel. Last year, DEA and Mexico teamed up to make the world's largest cash seizure exceeding $207 million, and Mexico made the largest-ever cocaine seizure of 23.6 metric tons. In addition, in September 2008, DEA led Project Reckoning that resulted in the arrests of over 600 individuals and seizure of over $70 million dollars from the notorious Gulf Cartel. The Gulf Cartel is alleged to be responsible for much of the violence that is currently occurring in Mexico. DEA has worked with Colombia to dismantle the major Colombian Cartels, to include the Norte Valle Cartel; with the arrests of Diego Montoya Sanchez and Juan Ramirez Abadia. Abadia was indicted in the United States in 2004, after being arrested in Brazil in August 2007, and extradited to the United States in August 2008. Sanchez was arrested in Colombia in September 2007 and is currently awaiting extradition to the United States. Colombian officials also arrested Otto Herrera-Garcia, a longtime Guatemalan drug trafficker and one of the most important targets in Central America. Herrera-Garcia is awaiting extradition to the United States after being arrested in Colombia in June 2007. A top AUC leader, Diego Fernando Murillo-Bejarano (a.k.a. Don Berna), was indicted in the U.S. in 2004, and surrendered to Colombian authorities in May 2005. He was extradited to the United States in May 2008 and pleaded guilty to drug trafficking in June. His sentencing is December 18, 2008.

FARC Commander Juan Jose Martinez Vega was arrested by Venezuelan police in May 2005 and immediately extradited to Colombia. In March 2006, he was indicted in the United States, and extradited here in April 2008, where he currently awaits trial.

Stride Methodology

The STRIDE (System to Retrieve Information from Drug Evidence) study conducted by DEA analyzed drug seizures and undercover purchases from April 2005 to September 2008. The study analyzed nearly 58,000 meth seizures and purchases, and over 24,000 cocaine seizures and purchases.

The data can be accessed at http://www.dea.gov

STRIDE is a database of drug exhibits sent to DEA laboratories from DEA, FBI, Customs and Border Protection, Immigration and Customs Enforcement, the United States Coast Guard, and the Washington Metro Police Department. STRIDE is not a representative sample of drugs available in the United States, but reflects all evidence submitted to DEA labs for analysis, and the data is not collected to reflect national market trends. However, STRIDE data reflect the best information currently available on changes in cocaine and meth prices and purity.

Source: DEA

****

BLOCK BEATER CALLER ID SERVICE: Information has surfaced recently regarding a company that is offering a service to the general public that will unblock any blocked telephone number. This service claims to be capable of obtaining and displaying any blocked telephone number, even law enforcement investigators who block their phone number during the course of their investigation.

Comment: Although this service was not designed to compromise law enforcement operations this potential exists. Officers should be aware of this service, especially if using a personal phone or allowing informants or agents to use an agency registered phone.

Source: Peel Regional Police Airport Division

****

TURNING YOUR CELL PHONE INTO A PERSONAL SAFETY DEVICE (RESOURCE): Imagine walking in a mall parking lot and seeing a suspicious van circling nearby. Just snap a photo of the van's license plate and send the photo to My Mobile Witness. This new cell phone service is designed to become a personal security device. My Mobile Witness stores photos or text and warehouses the information for the sole use by law enforcement authorities www.mymobilewitness.com. The technology is fast and simple to use: an individual takes a photo or creates a text message and sends it to their individual account where it is stored in the My Mobile Witness digital vault. The photo is time-stamped and stored on a secure site accessible only to law enforcement officials who have limited "active case" or subpoena access to the information when the images may be relevant. When an account holder sends a picture or text message it creates a record of their individual situation, to be used as a warning if someone later threatens them with harm.

Source: http://www.marketwatch.com/news/story/Turning-Your-Cell-Phone-Into/story.aspx?guid=%7B88A37137-B4C1-41DA-B05D-3FCC4D6BB373%7D via Washington Regional Threat and Analysis Center (WRTAC) December 17, 2008.

UNITED STATES: CUSTOMS PARTNERS WITH AIR CARRIERS TO HELP SPOT FRAUDULENT DOCUMENTS: U.S. Customs and Border Protection announced that 15,000 airline personnel have now been trained through its Carrier Liaison Program (CLP). The CLP was established in 2006 to enhance security by increasing carrier effectiveness in identifying improperly documented passengers destined for the United States. CBP's trainers engage in hands-on training in fraudulent document identification, passenger assessment, impostor recognition, and travel document verification. In fiscal year 2008, there were 5,665 carrier personnel trained during 124 missions in 30 countries throughout Europe, Asia, South America, and the Caribbean. There were two training missions to China, both prior to and following the summer Olympics. More than 1,100 airline and government officials received training in the cities of Beijing, Shanghai, Shenzhen, and Guangzhou.

Source: CBP, Office of Public Affairs, 24 November 2008

****

INCREASED SMART PHONE USE POSES POTENTIAL SECURITY RISK: Smart phones that link to server-based business e-mails or data files provide hackers with potential access past the inside perimeter component of a computer network's defense-in-depth security system. While few cases of security breaches involving smart phones have yet been documented, increasing government personnel reliance on smart phones could offer hackers access to government agencies' e-mail and data networks. Like the laptop and desktop computers whose functionality they increasingly mimic, smart, multifunctional phones are vulnerable to hackers.

- Most smart phone e-mail systems are not password-protected, which can provide backdoor access to the host organization's network. If a smart phone falls into the hands of a third party, he or she likely can access the owner's e-mail without authentication.

- Storing work-related information on a personal smart phone can make the phone a "rogue device that is difficult for an organization to protect because of the wide variety of phones and associated software in use." This situation potentially exposes the enterprise to an insider threat that could allow access to e-mail and data.

US–CERT and other cyber security experts recommend that smart phone users and system administrators minimize the risk posed by smart phone vulnerabilities as follows:

- Use virtual private networks to authenticate users and protect data in transit.
- Enforce strong passwords to access files or e-mail.
- Block access to public Wi-Fi.
- Practice strong physical security habits.
- Keep software and firmware up to date.
- Require device encryption systems.

Source: DHS Cyber Security – Volume 1, Number 11

****

THE DANGERS ASSOCIATED WITH SMOKING OXYCONTIN AND INDICATORS OF ITS USE

Overview

OxyContin was introduced in 1996 and is commonly known on the street as OC, OX, Oxy, Oxycotton, Hillbilly heroin, and kicker. A marked escalation of its abuse has been reported by drug abuse treatment centers, law enforcement personnel, and health care professionals. Although the diversion and abuse of OxyContin appeared initially in the eastern United States, it has now spread to the western United States, including Alaska and Hawaii. Oxycodone-related adverse health effects have increased markedly in recent years. (Source: DEA Website - http://www.usdoj.gov/dea/concern/oxycontin.html)

OxyContin tablets are a controlled-release oral formulation of oxycodone hydrochloride indicated for the management of moderate to severe pain when a continuous, around-the-clock analgesic is needed for an extended period of time. Approximately 50 percent of the OxyContin tablet consists of sugars and time release ingredients. The time-release component is a hydrocarbon that has a “greasy” characteristic (potential to coat the lungs). OxyContin is an opioid agonist and a Schedule II controlled substance that can be abused in a manner similar to other opioid agonists, legal or illicit. The time-release ingredients slow down the effects of the drug, but when the OxyContin® is smoked, the user feels the effects in about 5 seconds (similar to the crack cocaine “high”). The immediate “high” of OxyContin has an extremely strong addictive property. Additionally, Oxycodone HCl is highly acidic and chronic users may develop accelerated tooth decay - “meth mouth.” The Food and Drug Administration has strengthened the warnings and precautions sections in the labeling of OxyContin. There have been numerous reports of OxyContin® diversion and abuse in several states. Some of these reported cases have been associated with serious consequences, including death. (Source: Food and Drug Administration Website at http://www.fda.gov/cder/drug/infopage/oxycontin/)


Foil Used to Inhale OxyContin®


Foil Backside Heated

Smoking OxyContin

The OxyContin tablet can be ground into powder or left whole for smoking. However, if the tablet is ground, the charred residue appears as spots. Normally, the user rinses or rubs off ("sucks off") the tablet coating before igniting the drug or "chasing the dragon." The phrase similarly is used to describe opium and heroin use. Burning OxyContin® produces copious smoke, and the user puts his/her head over the smoke to inhale the fumes. The smoker may use a straw or tube to get a more direct concentration of the smoke. Pipes could be used to prevent loss of drug fumes, but normally are not, due to the high temperatures at which Oxycodone burns. The open foil provides a cooling effect and avoids burning the users' lips. Individuals with legal prescriptions of OxyContin® do not perceive the "smoking" of OxyContin illegal; the method simply produces the effects of the drug more rapidly than oral ingestion. The danger lies in the difficulty of controlling the amount of the drug that is inhaled leading to a high potential for overdose.

DEA San Diego Case

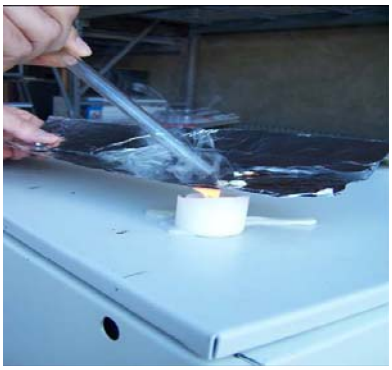
In late October 2008, the DEA San Diego, California, Field Division initiated an investigation involving a suspected distributor of OxyContin® in Southern California. The target was distributing the OxyContin tablets from his residence in Poway, California. After a series of controlled purchases of the drug ($60.00/tablet 80-OC) from the suspect, a search of the suspect's residence and vehicle produced the subject's arrest and the seizure of over 20 OxyContin® tablets, a variety of pills including Valium and Buprenorphine, gram-quantities of hashish /marijuana, and paraphernalia such as aluminum foil, a grinder, a pill splitter, a scale, prescription bottles, and syringes. Pieces of foil containing drug residue resembling magic marker lines/tracks (photos shown above) were seized from the vehicle and sent to the DEA Southwest Laboratory for analysis. Burnt drug residue on pieces of foil tested positive for Oxycodone. (Source: DEA San Diego, CA Field Division)

Officer Alert

According to a chemist at the DEA Southwest Lab, a field test for Oxycodone would not be accurate, since the overwhelming majority of the tablet vaporizes during the smoking process.

Testing of the drug indicates that Oxycodone HC1 burns at about 275 C compared to methamphetamine HCl (175 C) and cocaine base (100 C). The decomposition of the Oxycodone is a viable risk, since OxyContin burns and melts at such high temperatures. However in this case, the Oxycodone remained intact.

The photograph on the right depicts the process of “chasing the dragon.” A chemist at the DEA Southwest Lab wiped off the outer green coating of the OC80 (Purdue Pharma) tablet, placed it on a piece of aluminum foil, and heated it using a candle. The vapors that were emitted would have been inhaled using a tube or some sort of pipe. In the lab, it showed that Oxycodone vapors would survive this heating process and were in fact analyzed using mass spectrometry. The other components in the tablet, the sugars and time release materials, also vaporize and would be inhaled as well. The picture below (bottom left) shows the streak or "skid" that would result in the process of melting the tablets. The other picture shows the skid marks, which were confirmed to contain Oxycodone residue.



Comment: If you have any comments in reference to this report, please contact the EPIC Research and Analysis Section, Tactical Bulletins Unit, I/A Monika Barnum at (915) 760-2747, or Unit Chief Nancy Thompson at (915) 760-2105.

Source: DEA San Diego Field Division

****

NATIONAL DRUG THREAT ASSESSMENT 2009: The trafficking and abuse of illicit drugs inflict tremendous harm upon individuals, families, and communities throughout the country. The violence, intimidation, theft, and financial crimes carried out by drug trafficking organizations (DTOs), criminal groups, gangs, and drug users in the United States pose a significant threat to our nation. The cost to society from drug production, trafficking, and abuse is difficult to fully measure or convey; however, the most recent data available are helpful in framing the extent of the threat. For example:

- More than 35 million individuals used illicit drugs or abused prescription drugs in 2007.
- In 2006 individuals entered public drug treatment facilities more than 1 million times seeking assistance in ending their addiction to illicit or prescription drugs.
- More than 1,100 children were injured at, killed at, or removed from methamphetamine laboratory sites from 2007 through September 2008.
- For 2009 the federal government has allocated more than $14 billion for drug treatment and prevention, counterdrug law enforcement, drug interdiction, and international counterdrug assistance.
- In September 2008 there were nearly 100,000 inmates in federal prisons convicted and sentenced for drug offenses, representing more than 52 percent of all federal prisoners.
- In 2007 more than 1.8 million drug-related arrests in the United States were carried out by federal, state, and local law enforcement agencies.
- Mexican and Colombian DTOs generate, remove, and launder between $18 billion and $39 billion in wholesale drug proceeds annually.
- Diversion of controlled prescription drugs costs insurance companies up to $72.5 billion annually, nearly two-thirds of which is paid by public insurers.

DTOs rapidly adapt to law enforcement and policy initiatives that disrupt their drug trafficking operations. Law enforcement and intelligence reporting revealed several strategic shifts by DTOs in drug production and trafficking in 2007 and early 2008, attributed in part to the success of counterdrug agencies in disrupting the operations of DTOs. Many of these shifts represent immediate new challenges for policymakers and resource planners.

The entire assessment can be found at: http://www.usdoj.gov/ndic/pubs31/31379/31379p.pdf

Source: National Drug Intelligence Center

****

HOTELS NEED TO BE PREPARED FOR DISASTER SITUATIONS: The terrorist attack in India has proven the need for security and disaster preparedness plans for hotels. Preparedness may not prevent or protect from disasters; however, it may help to prepare hotel staff to deal more effectively with disaster or terrorist situations. Front line hotel employees should be trained to take control of disaster situations by directing guests to exit routes or reassuring them that the situation is being handled in the best possible way. Good communication plans are a necessity; therefore, having staff trained to quickly and accurately disseminate information may greatly benefit the outcome of the situation. Hotels must incorporate a critical incident plan in

order to be able to successfully resolve emergencies such as shootings, bomb threats, hostage situations, or natural disasters. Local 911 centers, first responders, and other emergency personnel should be involved and have access to critical information, such as floor plans. Hotel managers must be able to 'lock down' their facilities and notify all guests on emergency procedures. Lock downs can limit the number of guests exposed to violent situations and keep guests out of the way of emergency personnel. Having good critical incident plans in place is vital to hotels and the successful resolution of disaster situations.

Source: Institute for Preventive Strategies Open Source Daily Brief

****

NUMBER OF LAW ENFORCEMENT OFFICERS KILLED IN THE UNITED STATES FALLS SHARPLY IN 2008: The number of officers killed in the line of duty fell sharply this year when compared with 2007, and officers killed by gunfire reached a 50-year low. Based on analysis of preliminary data, the National Law Enforcement Officers Memorial Fund (NLEOMF) and Concerns of Police Survivors (C.O.P.S.) found that 140 officers have died in the line of duty so far this year. That is 23 percent lower than the 2007 figure of 181, and represents one of the lowest years for officer fatalities since the mid-1960s. This year's reduction includes a steep, 40 percent drop in the number of officers who were shot and killed, from 68 in 2007 to 41 in 2008. The last time firearms-related fatalities were this low was 1956, when there were 35 such deaths. The 2008 figure is 74 percent lower than the total for 1973, when a near-record high 156 law enforcement officers were shot and killed. In 2008, for the 11th year in a row, more law enforcement officers, 71, died in traffic-related incidents than from gunfire or any other single cause of death. Mirroring the nationwide drop in traffic fatalities among the general public this year, the number of officers killed in traffic incidents was down 14 percent from 2007. Last year, record high 83 officers died on our roadways. Among other causes of death, 17 officers succumbed to job-related physical illnesses, three died in aircraft accidents, two were fatally stabbed, two died in bomb-related incidents, and one each was beaten to death, drowned, accidentally electrocuted and died in a train accident. NLEOMF Chairman and CEO Craig W. Floyd cited a number of reasons for the sharp decline in officer fatalities this year: 1) better training and equipment, plus a realization among officers that "every assignment is potentially life-threatening, no matter how routine or benign it might seem;" 2) increased use of less-lethal weaponry, including TASER stun guns, which allow officers to apprehend resisting violent offenders with less chance of assault or injury; 3) more officers wearing bullet-resistant vests-over the past 20 years; 4) a downturn in violent crime-the Department of Justice reported that violent crime is at its lowest level since 1973; and 5) a tougher criminal justice system, with a record 2.3 million offenders in correctional facilities nationwide.

For more information refer to the following link: http://www.nleomf.com/TheMemorial/Facts/2008_endyear_report.pdf

Source: National Law Enforcement Officers Memorial Fund

WRTAC Customer Satisfaction Survey

Return to: Washington Regional Threat Analysis Center
Washington, D.C.
202-233-1472 (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.

Comments: _____