



UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including Schools and Universities\)](#)

[International](#)

[Information Technology and Telecommunications](#)

[Banking and Finance Industry](#)

[National Monuments and Icons](#)

[Chemical and Hazardous Materials Sector](#)

[Postal and Shipping](#)

[Commercial Facilities](#)

[Public Health](#)

[Communications Sector](#)

[Transportation](#)

[Critical Manufacturing](#)

[Water and Dams](#)

[Defense Industrial Base Sector](#)

[North Dakota Homeland Security Contacts](#)

[Emergency Services](#)

NORTH DAKOTA

First responders from 12 counties do two-part exercise to prepare for potential disaster. First responders from a 12-county area gathered in Jamestown, North Dakota, February 15, to figure out how to handle a serious chemical spill. The officials were participating in Operation Roughrider, a two-part exercise at the Jamestown Civic Center designed to help them prepare for a large-scale disaster requiring the cooperation of police, fire and ambulance agencies from around the region. The drill was divided into two parts. "This morning we started with a functional exercise to test the inter-operative operations of the communications," said a training and exercise officer for the North Dakota Department of Emergency Services. "The second part is a table-top exercise where the first responders discuss issues around a catastrophic hazardous materials spill in Jamestown." Source: <http://www.jamestownsun.com/event/article/id/129657/>

Commissioner questions reliability of Xcel's infrastructure. A North Dakota regulator said the prolonged Xcel power outage the weekend of February 12 in parts of Fargo and West Fargo raises questions about whether the utility has kept up its infrastructure. A member of the North Dakota Public Service Commission noted Xcel has had several power failures or surges in Fargo and Grand Forks in recent months. "I think it raises the larger issue: How old is the Xcel infrastructure, and is it time to upgrade the system?" An Xcel spokeswoman, said the system overall remains "very reliable." Meanwhile, investigators February 14 continued to delve into the power failure, which affected an estimated 16,000 customers in Fargo and West Fargo. The failure stemmed from equipment failure at a power substation at Main Avenue and 45th Street in Fargo. Xcel is investigating to determine whether any customers experienced power surges associated with the failure. Repairs to the damaged substation continue, along with the investigation. Source: <http://www.inforum.com/event/article/id/308733/>

Jamestown won't pay for flood damage. The city of Jamestown, North Dakota, will no longer pay for damage to private property from flooding, dikes, or levees. The city administrator said that after spring flooding in 2009, the city paid about \$500,000 to cover damage. The mayor said it was a financial burden. The city council recently approved a policy denying city liability. Source: http://www.bismarcktribune.com/news/state-and-regional/article_806eba74-37fa-11e0-a874-001cc4c03286.html

REGIONAL

Nothing Significant to Report

NATIONAL

Smartphone users not aware of mobile security risks. More than a third of surveyed smartphone users are not aware of the increasing security risks associated with using their phones for financial

UNCLASSIFIED

purposes and to store personal data, according to a new survey by AVG and the Ponemon Institute. The study also showed that just 29 percent of surveyed smartphone owners have considered downloading free or paid anti-virus software to help protect their most personal devices. The survey targeted 734 U.S. consumers over the age of 18 who own a smartphone such as an iPhone, Blackberry, or Android device. Surveyed consumers also expressed a lack of awareness in respect to a number of key security issues faced by smartphone users. Source: <http://www.net-security.org/secworld.php?id=10609>

U.S. investigators in Mexico to assist in hunt for U.S. agents' assailants. The first of at least a dozen U.S. investigators departed for Mexico February 16 to assist in the hunt for unidentified gunmen who killed a U.S. special agent and wounded another in a roadside attack February 14. DHS announced the creation of a joint task force with the Justice Department to assist in the investigation. The Immigration and Customs Enforcement (ICE) agent died from his gunshot wounds. He was assigned to the agency's Laredo, Texas, office and was on loan to the U.S. Embassy in Mexico City. The deceased agent's injured partner was moved to a hospital in Houston for treatment and debriefing. He was later released. The two agents were returning to Mexico City after meeting with U.S. personnel in the state of San Luis Potosi, ICE said. Earlier, officials had said the two were on their way to Monterrey City. A key question facing investigators is whether the agents were targeted because of their jobs or were random victims of drug traffickers who may have wanted their SUV. A senior U.S. official said the investigation is ongoing. According to a U.S. Representative from Texas, the two ICE agents "were pursued by numerous cartel members and run off the road while driving a U.S. government vehicle with diplomat license plates. When the agents identified themselves as American diplomats, the cartel members responded by opening fire." Source: <http://www.bellinghamherald.com/2011/02/16/1872005/us-investigators-in-mexico-to.html>

INTERNATIONAL

Iran tries internet censorship, execution as protesters demand democracy. After pro-democracy protests in Tehran, Iran, February 14, Iranian authorities have started blocking pro-opposition Web sites and electronic media, and greatly slowed broadband speed in major cities. Text-message and mobile-phone traffic was disrupted, and the word "bahman", the current month in the Persian calendar, has been blocked. Authorities have tried to censor the actual protests and reporting of the events, blocking the top two news sites and jamming satellite TV broadcasts and prohibiting photography. Conservative lawmakers have also called for the execution of two opposition leaders who asked for permission to demonstrate but were denied and did it anyway. Source: http://nymag.com/daily/intel/2011/02/iran_tries_internet_censorship.html

Gunmen kill top police commander in Mexico. Gunmen ambushed and killed a top police commander and then set his car on fire in the northern Mexican border state of Nuevo Leon, authorities said February 14. His body was found February 13 inside a smoldering car abandoned in Monterrey, the state government said in a statement. Monterrey is the capital of Nuevo Leon and Mexico's third-largest city. The victim was the director of the state's intelligence and security center, a job he had taken in August. He was shot at least five times, the statement said. Local news media reported that the commander, who was the nephew of the former state public safety secretary, had

UNCLASSIFIED

UNCLASSIFIED

been kidnapped hours earlier as he left his home. Source:

<http://www.npr.org/templates/story/story.php?storyId=103181125>

Taliban suicide bomber strikes Kabul mall. A Taliban suicide bombing February 14 ripped apart the entrance to the sole Western-style shopping mall in Kabul, Afghanistan, killing at least two security guards. The Taliban quickly took credit for the strike at the City Center mall, which adjoins a four-star hotel popular with foreigners. The attack targeted the same demographic groups as last month's bombing in a high-end Kabul supermarket: Western civilians and the Afghan elite with whom they most often mix. While Kabul's expatriate community and prominent Afghans have been attacked by the Taliban in the past, the capital had enjoyed months of calm in the second half of 2010 even as violence spiked up elsewhere in the country. The bombings also appear to be signaling a strategy shift by the Taliban, who in early January said they planned to focus more on Kabul. The entrance to the City Center mall was a crush of broken glass and mangled aluminum siding. Windows were blown out of nearby shops and some parts of the hotel's glass facade. Source:

http://online.wsj.com/article/SB10001424052748703584804576144084115745532.html?mod=googlenews_wsj

Gunmen kill 8 in violent north Mexico border city. Gunmen barged into a bar in Ciudad Juarez, Mexico, and opened fire February 10, killing seven women and one man, authorities said. Three other people were wounded at the "Las Torres" bar and were in critical condition, a spokesman for Chihuahua state prosecutors said. The attack is under investigation. More than 3,000 people were killed last year in Ciudad Juarez, the city of 1.3 million residents across the border from El Paso, Texas. Source:

http://www.google.com/hostednews/ap/article/ALeqM5g1jzxkq4eN6VQ_9_DPpwyWi0HMIA?docId=780770f73e6b4d8690ca467fee4df15e

Mexican club attack kills 6. Armed men opened fire and hurled a grenade into a crowded nightclub February 12, killing 6 people and wounding at least 37 in Guadalajara, Mexico, whose former tranquility has been shattered by escalating battles among drug cartels. The attack in Mexico's second-largest municipality took place just hours after a shootout between soldiers and presumed cartel gunmen left eight people, including an innocent driver, dead in the northeastern city of Monterrey. In the Guadalajara attack, assailants in a Jeep Cherokee and a taxi drove up to the Butter Club, located in a bar and restaurant district popular with young people, and sprayed it with bullets. Some of the men got out of the taxi and threw a grenade into the nightclub entrance, a police official said. The gunmen fled after the predawn attack. Source:

http://www.denverpost.com/nationworld/ci_17374997

BANKING AND FINANCE INDUSTRY

Visa incents 'Dynamic Authentication'. A move toward Europay, Mastercard and Visa (EMV) integrated circuit cards can help merchants cut their security compliance costs, but only if they operate outside the United States, is the message from Visa Inc., which the week of February 7 announced the launch of the Visa Technology Innovation Program. It is designed to eliminate eligible international merchants from annual validations of compliance with the Payment Card Industry Data Security Standard. In the United States, where no official movement toward the EMV standard exists, other types of dynamic authentication are being encouraged by Visa. But they will not offer the same

UNCLASSIFIED

UNCLASSIFIED

incentives (i.e. eliminating compliance validations) the Technology Innovation Program provides to qualifying EMV-compliant merchants in other parts of the world. "With the United States facing government price controls on debit and restrictive routing and exclusivity rules, it is not feasible or appropriate to drive the market toward major infrastructure investments, especially in an environment where financial institutions could lose billions in revenue as a result of the regulation," Visa's group executive for the Americas said in a statement issued by Visa. "With such a dramatic potential for revenue loss, financial institutions will likely curtail investments in future innovations." Source: http://www.bankinfosecurity.com/articles.php?art_id=3351

New scam targets online sellers. The FBI's cyber complaint center has released a report warning about a new scam targeting sellers on online marketplace Web sites. According to IC3, the ploy generates fake receipts through an executable file circulating on hacking forums recently, the center said. The generator asks the would-be victim to disclose information about item name, price, and the date the order was taken. As soon as the victim hits "Generate," an HTML file is created in the program folder. The program makes what appears to be a legitimate marketplace receipt and a copy of the "Printable Order Summary," similar to documents resulting from legitimate marketplace purchases. Details, such as "Total before tax" and "Sales tax," make the receipt extra convincing. According to IC3, many sellers on these online markets will ask the buyer to send them a copy of the receipt in the event of missing orders or any other issues that may arise during or after the Web transaction. Source: <http://www.thenewnewinternet.com/2011/02/14/new-scam-targets-online-sellers/>

Treasury identifies Lebanese Canadian bank SAL as a 'primary money laundering concern'. The U.S. Department of the Treasury announced February 10 the identification of The Lebanese Canadian Bank SAL together with its subsidiaries (LCB) as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act (Section 311) for the bank's role in facilitating activities of an international narcotics trafficking and money laundering network. This network moves illegal drugs from South America to Europe and the Middle East via West Africa and launders hundreds of millions of dollars monthly through accounts held at LCB, as well as through trade-based money laundering involving consumer goods throughout the world, including used car dealerships in the United States. Treasury has reason to believe LCB managers are complicit in the network's money laundering. The action also exposes the terrorist organization Hezbollah's links to LCB and the international narcotics trafficking and money laundering network. "This action seeks to protect the U.S. financial system from the illicit proceeds flowing through LCB and to deprive this international narcotics trafficking and money laundering network of its preferred access point into the formal financial system," said the Under Secretary for Terrorism and Financial Intelligence. "Any financial institution that collaborates in illicit conduct on this scale risks losing its access to the United States." Source: <http://www.treasury.gov/press-center/press-releases/Pages/tg1057.aspx>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Radioactive material thefts decline. Incidents of missing radioactive materials are dropping dramatically, easing concerns of extremists detonating crude, low-level radioactive "dirty bombs" to sow panic. The Canadian Nuclear Safety Commission (CNSC) reported that five radioactive sources, typically found in measuring and analytical equipment, were lost or stolen last year and five more in 2009. That compares with a 2005-08 annual average of 15, with a record 21 missing devices in 2007.

UNCLASSIFIED

UNCLASSIFIED

The news softens previous criticism about the effectiveness of federal controls over nuclear materials. Under pressure to improve its vigilance, the commission in 2006 became the first nuclear regulator in the world to implement a national registry and sealed source tracking system, where thousands of businesses and institutions are required to report to on the status of their CNSC-licensed nuclear devices. "Licensees have become more aware of the importance of maintaining accurate inventories, and understand CNSC expectations and the level of importance placed on safety and security of all sealed sources," the agency said in a February 11 statement, adding more than 1,400 inspections are done annually at sites with high-and medium-risk sources. Six sources remain missing from 2009-2010, but all are rated at low or very low risk for potential harm to human health. Very high risk sources have never been reported missing in Canada. Source:

<http://www.ottawacitizen.com/news/Radioactive+material+thefts+decline/4271185/story.html>

COMMERCIAL FACILITIES

(Texas) HEB store evacuated after bomb threat. An HEB store on the Far West Side in San Antonio, Texas, was evacuated February 16 after a threatening note was found. An employee found the note around 9 a.m. Officials said the note warned that there were explosives throughout the store, and demanded money be left within a certain time frame. About 200 people were evacuated, and bomb sniffing dogs were brought in to check the store. Investigators were able to identify a 30-year-old man as the man they said left the threatening note after reviewing security video. Officers then tracked the man down at his house. News 4 WOAI was told that, although he first denied being responsible, the man later confessed and said someone told him to leave the note for \$100. The store was reopened after it was determined there were no explosives inside. Source:

<http://www.woai.com/news/local/story/HEB-store-evacuated-after-bomb-threat/4xGRr8vLRUekZEdvY-3wyg.csp>

COMMUNICATIONS SECTOR

Hackers create WiFi content spoofing device. A pair of creative hackers have built a device capable of connecting to wireless networks and altering the Web content users access, as part of a project to demonstrate how news can be manipulated. The device mimics a pass-through power socket, making it hard to observe, and has already been tested in cafe shops in Berlin, Germany, where its creators are based. Inside the 12-centimeter long casing is a small circuit board with an Atheros chipset and an antenna. It runs a customized Linux distribution designed for embedded systems. When turned on, the device automatically searches for wireless networks and connects using passwords supplied in advance. A reverse SSH tunnel is established with a remote server, allowing attackers to control the device from a distance. The tunnel uses 2048-bit encryption and is routed over Tor nodes, making it virtually impossible to determine where the attacker is located. The device launches Address Resolution Protocol spoofing attacks to position itself as a gateway between the other wireless clients and the real router. This allows attackers to manipulate content passing through it. Combined with other techniques, especially on open wireless networks, the device can also be used to hijack users' sessions, read e-mails, and perform other attacks. Source:

<http://news.softpedia.com/news/Researchers-Demo-WiFi-News-Spoofing-Device-184549.shtml>

UNCLASSIFIED

UNCLASSIFIED

FCC asks for money for direction-finding gear. The Federal Communications Commission (FCC) wants to equip its enforcement agents with better gear. In the budget submitted to Congress by the U.S. President, the FCC asked for \$350,000 for portable direction-finding gear. It said that the current equipment used by the enforcement bureau's field offices to identify and resolve interference, provide limited portable or semi-fixed capability for direction finding. Source:

<http://www.radioworld.com/article/113834>

The cyberweapon that could take down the Internet. A new cyberweapon could take down the entire Internet – and there is not much current defenses can do to stop it. So say a student at the University of Minnesota (UM) in Minneapolis and his colleagues, the masterminds who have created the digital ordnance. They are suggesting improvements to its defenses. The students' new attack pits the structure of the Internet against itself. Hundreds of connection points in the net fall offline every minute, but it goes unnoticed because the net routes around them. It can do this because the smaller networks that make up the Internet, known as autonomous systems, communicate with each other through routers. When a communication path changes, nearby routers inform their neighbors through a system known as the border gateway protocol (BGP). These routers inform other neighbors in turn, eventually spreading knowledge of the new path throughout the Internet. A previously discovered method of attack, dubbed ZMW – after its three creators, U.S. researchers who came up with their version 4 years ago – disrupts the connection between two routers by interfering with BGP to make it appear the link is offline. The UM student and his colleagues worked out how to spread this disruption to the entire Internet and simulated its effects. Source:

<http://www.newscientist.com/article/dn20113-the-cyberweapon-that-could-take-down-the-internet.html>

FCC acts against cell phone jamming. The enforcement arm of the Federal Communications Commission (FCC) has launched a new effort to crack down on cell phone and GPS jamming devices. The FCC Enforcement Bureau warned consumers, manufacturers, and retailers, including online and Web-only companies, that the marketing, sale, or use of cell, GPS, and other jamming devices is illegal. The Enforcement Bureau chief said plans include education, outreach, and aggressive enforcement. Jamming devices are radio frequency transmitters that intentionally block, jam, or interfere with wireless communications. Increasingly, online retailers tout small, inexpensive jammers as the solution for noisy classrooms, theaters, restaurants, or business meetings. But jammers are indiscriminate and can block critical public safety and other emergency communications. Source:

<http://www.wsbt.com/business/wsbt-fcc-acts-against-cell-phone-jamming-20110212,0,4312719.story?>

CRITICAL MANUFACTURING

General Motors recalling more than 50,000 CTS vehicle. General Motors Co. (GM) is recalling more than 50,000 Cadillac CTS cars made in Lansing, Michigan. The 2009 and 2010 model-year vehicles are under recall because of a problem that could destabilize a rear wheel and make the car difficult to steer. Of the recalled vehicles, about 44,000 were made in the United States in 2009 and 2010. The CTS problem lies in the rear toe link assembly, according to the Detroit, Michigan-based automaker's filing with the National Highway Traffic Safety Administration. The filing said a wax coating on a nut could cause it to come loose, creating a metal clanking noise. The loose part could result in a sudden

UNCLASSIFIED

UNCLASSIFIED

change in the vehicle's handling and a driver might not be able to control the vehicle. No injuries or deaths have been reported because of the problem, GM said. The vehicles under recall were built between June 16, 2008, and April 20, 2009. Owners of the affected vehicles will be notified soon through recall letters. Source:

<http://www.lansingstatejournal.com/article/20110217/BUSINESS01/102170321/General-Motors-recalling-more-than-50-000-CTS-vehicles?odyssey=tab|mostpopular|text|FRONTPAGE>

Honda recalls 97,000 Fit subcompacts in the U.S. Honda Motors is recalling 97,000 Fit subcompact cars in the United States because of engine component problems. The Japanese automaker said February 16 it needs to replace a part called a lost-motion spring, which is a component in the engine valve train, in 2009 and 2010 models of the small car. No crashes or injuries have been reported related to this problem. The company said the lost-motion springs, which are compressed by rocker arms in normal engine use, may bend or break over time, resulting in abnormal noise and potentially causing engine damage or stalling. Honda said owners of Fit vehicles should take them to Honda dealers to replace the part after they receive notifications in the mail, which will be sent out in early March. Source:

[http://money.cnn.com/2011/02/17/autos/honda_recall/index.htm?section=money_topstories&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:rss/money_topstories+\(Top+Stories\)](http://money.cnn.com/2011/02/17/autos/honda_recall/index.htm?section=money_topstories&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:rss/money_topstories+(Top+Stories))

DEFENSE/ INDUSTRY BASE SECTOR

U.S. to replace nuke delivery platforms. The U.S. Presidential administration's fiscal 2012 budget request calls for the United States to replace the land-, air-, and sea-based components of its nuclear deterrent, potentially setting the nation on a course that could cost hundreds of billions of dollars over 5 decades, Time magazine reported. The administration rolled out its budget February 14 for the fiscal year that begins October 1. The move toward replacing all three components of the nation's nuclear "triad" stems from the conclusions of the administration's Nuclear Posture Review, which asserted "retaining all three triad legs will best maintain strategic stability at reasonable cost, while hedging against potential technical problems or vulnerabilities." Source:

http://www.globalsecuritynewswire.org/gsn/nw_20110214_1414.php

(Texas) Report says NASA underestimated shuttle dangers. NASA seriously underestimated the dangers astronauts faced when the shuttle fleet began flying in the early 1980s, an internal safety study shows. At the time, managers thought there was only a 1-in-100,000 chance of losing a shuttle and its crew. Engineers thought the probability was closer to 1 in 100. But in reality, the odds of a disaster were much higher. On each of the shuttle's first nine missions, there was a 1-in-9 chance of a catastrophic accident, according to the new risk analysis. On the next 16 flights that led up to and included the January 1986 Challenger disaster, the odds were 1 in 10. NASA lost 14 astronauts in 2 shuttle tragedies, and saw near misses on a dozen other flights. NASA's Shuttle Program Safety and Mission Assurance Office at Johnson Space Center in Houston, Texas, performed the assessment to gauge the progression of risk — increases and decreases — over 3 decades of fleet operations. Doing so could help next-generation rocket and spaceship operators better understand the real level of risk involved in flying astronauts on inherently dangerous missions. Source:

<http://www.militarytimes.com/news/2011/02/gannett-nasa-report-says-shuttle-dangers-underestimated-021311w/>

UNCLASSIFIED

EMERGENCY SERVICES

(West Virginia) Deputy U.S. Marshal gunned down in West Virginia. A deputy U.S. Marshal was shot and killed while serving an arrest warrant at a West Virginia home February 16, according to a U.S. Marshals Service spokesman. A total of three deputies were hit by a shotgun blast as they entered a home in Elkins at about 8:30 a.m., the spokesman said. The deputies had been serving an arrest warrant for a 50-year-old man, who was wanted on a charges related to possession of cocaine with the intent to distribute. The suspect and the officers exchange fire, and the suspect was killed. One deputy “continues to recover from his injuries,” and the third has been treated at nearby hospital and released, the spokesman added. At least one state police officer was also at the scene of the shooting, but was not injured, according to a West Virginia State Police spokesman. Source: <http://www.cnn.com/2011/CRIME/02/16/west.virginia.shooting.marshals/?hpt=T2>

Gunmen kill US agent, wound another, in Mexico. A U.S. Immigration and Customs Enforcement (ICE) agent on assignment to the ICE Attache in Mexico City, Mexico from his post in Laredo, Texas, died February 15 when gunmen attacked his blue Suburban vehicle in the northern state of San Luis Potosi. A second ICE agent was shot in the arm and leg and was in stable condition, according to statements from the Department of Homeland Security. The Homeland Security Secretary said the fatal attack on American law enforcement, the highest-profile attack since the 1985 torture and killing of a Drug Enforcement Administration agent, will not change the U.S. commitment to supporting Mexico in its crackdown on organized crime. The two agents were driving on a four-lane, federal highway between Mexico City and Monterrey when they were stopped at what may have appeared to be a military checkpoint, according to one Mexican official. Mexican military officers said they had no checkpoints in the area. After they stopped, someone opened fire on them, the official said. Police said a checkpoint was unlikely on such a high-speed stretch of highway and that the bullet-riddled Suburban was found off to one side of the road. The United States has increased equipment and training support for Mexico in recent years through its \$1.4 billion Merida Initiative. Source: http://news.yahoo.com/s/ap/20110216/ap_on_re_la_am_ca/lt_mexico_ice_agents_shot

U.S. icebreakers can't handle Alaska oil spills: official. The U.S. Coast Guard does not have enough working icebreakers to respond to a major oil spill in Alaskan waters, the top official who oversaw the containment of the BP oil spill warned Congress February 11. “The current condition of the Coast Guard icebreaker fleet should be of great concern to the senior leaders of this nation,” the general testified at a House Transportation subcommittee hearing on the 2010 oil spill in the Gulf of Mexico. He said two of the three ice breakers do not work, and decisions on future funding for the fleet continued to be delayed. Similar concerns about icebreakers were raised by the special presidential commission that looked into the BP oil spill and government offshore drilling regulations. He said current infrastructure is inadequate to support extensive response and recovery operations off Alaska’s North Slope, except for oil industry facilities at Dead Horse and Prudhoe Bay. “Point Barrow, the only location close to the new Beaufort and Chukchi Sea lease areas, has limited access and no ability to support large-scale operations,” he said. Source: <http://www.reuters.com/article/2011/02/11/us-arctic-oil-vessels-idUSTRE71A5RM20110211?feedType=RSS&feedName=domesticNews>

ENERGY

PHMSA says states, feds must 'step up' gas pipeline safety together. State and federal regulators must work together to increase public confidence after a string of natural gas pipeline explosions, the deputy administrator of the U.S. Pipeline and Hazardous Materials Safety Administration (PHMSA) said February 14. "I intend to lead a push for better-quality risk assessment and records management. If you don't know what you have in the ground, it's often hard to manage the risk of that," the deputy administrator said. The gas pipeline industry was already facing scrutiny for last year's deadly explosion on a Pacific Gas and Electric transmission line in San Bruno, California, before a trio of recent blasts heightened the attention. PHMSA's associate administrator for pipeline safety, called the Allentown, Pennsylvania, and San Bruno, California, blasts "major tragedies," but added the public should not overlook significant progress made by the pipeline industry in the past decade to adopt PHMSA's integrity management program. Source:

<http://www.platts.com/RSSFeedDetailedNews/RSSFeed/NaturalGas/6830613>

(Pennsylvania) Pipe 'imperfection' found after fatal blast in Pennsylvania. Investigators looking into the cause of a gas explosion that killed five people in Allentown, Pennsylvania the week of February 7 are focusing on an "imperfection" in a pipe near the blast site. The February 9 explosion flattened a pair of row houses and set fire to a block of homes, killing five people. On February 12, investigators told the Morning Call of Allentown they were zeroing in on an abnormality in a section of pipe. An area fire chief said workers were to dig up the section of pipe February 13 and take a closer look. The Pennsylvania Public Utility Commission will then send the pipe to a forensics expert. A spokesman for UGI Utilities Inc. said the commission is running the inspection and will report to the National Transportation Safety Board. Source:

http://www.pennlive.com/midstate/index.ssf/2011/02/pipe_imperfection_found_after.html

Alaska oil pipeline has safety and environmental risks. The U.S. Department of Transportation's pipeline safety division said the trans-Alaska pipeline is corroded and poses a severe public safety and environmental risk. The 800-mile pipeline ships 12 percent of the domestic oil supply. In a letter sent earlier in February to the Alyeska Pipeline Service Co., a coalition of oil companies that control the pipe, the Pipeline and Hazardous Materials Safety Administration [PHMSA] said "multiple conditions pose a pipeline integrity risk." A reason for the increased corrosion is limited use. At its peak, the pipeline carried 2.1 million barrels per day, crossing three mountain ranges, from the North Slope of Alaska to Valdez, the state's northernmost port. The decrease in oil flow is accompanied by a drop in crude oil temperatures, which leads to corrosion. The lower temperatures also create the risk the water mixed with crude oil may freeze in case the pipeline needs to be temporarily shut down. The PHMSA letter said, "the water itself is another corrosion hazard" that could damage all components of the pipeline including instrumentation and valves. Source:

<http://www.csmonitor.com/Environment/2011/0212/Alaska-oil-pipeline-has-safety-and-environmental-risks>

FOOD AND AGRICULTURE

USDA uncovers scheme to import fake Chinese organic food. On February 11, the U.S. Department of Agriculture (USDA) February 11 publicly released evidence of attempted fraud by a Chinese organic agricultural marketer. The agency's National Organic Program (NOP) made public a fraudulent organic certificate produced by an uncertified supplier in China. The Chinese firm used the counterfeit certificate to represent non-organic crops, including soybeans, millet, and buckwheat, as certified organic. A French USDA accredited certifying agent whose name was illegally used on the fraudulent document, brought this issue to the attention of NOP officials. Source:

<http://westernfarmpress.com/management/usda-uncovers-scheme-import-fake-chinese-organic-food>

(Florida) Mediterranean fruit flies found in Pompano Beach. The Florida Department of Agriculture and Consumer Services (FDACS) has positively identified the presence of two Mediterranean fruit flies, *Ceratitis capitata*, collected during routine fruit fly monitoring. The origin of these flies, collected in Pompano Beach residential area of Broward County, has not been determined. The department is placing 2,000 additional traps in a 50-square-mile area around the positive find and with the U.S. Department of Agriculture will check the traps daily. In addition, the department will set up a certification process for host materials to move in and out of the quarantine zone. The Mediterranean fruit fly (Medfly) is considered the most serious of the world's fruit fly pests due to its potential economic harm and threat. It attacks more than 250 different fruits, vegetables and nuts, including oranges, grapefruit, lemons, apples, guava, mango, tomatoes, and peppers. Source:

<http://southeastagnet.com/2011/02/11/mediterranean-fruit-flies-found-in-pompano-beach/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(North Carolina) Kinston National Guard Armory struck in weekend b&e. A breaking and entering at a National Guard Armory in Kinston, North Carolina, is under investigation. Deputies with the Lenoir County Sheriff's Office said an armory official told them the motor pool building had been broken into over the weekend of February 12 and 13. Numerous items were reported stolen, including cash from a lock box/money box, fuel cards, and a uniform. Several laptop computers were taken as well as a flat screen TV. A vending machine was broken into and a heavy duty steam/pressure washer was taken from the building. The value of the missing items is estimated to be \$4,500. The only clues to what may have happened were a set of wheel tracks leading from the motor pool building to a fence on the rear corner of the property, where a large hole was found cut out in the fence. Source:

<http://www2.wnct.com/news/2011/feb/16/kinston-national-guard-armory-struck-weekend-be-ar-788664/>

(Wisconsin) Girl, 14, arrested in Racine school bomb threat. Police in Racine, Wisconsin, arrested a 14-year-old girl in a bomb threat February 15 at McKinley Middle School, where she is a student. Police were called on a report of bomb threat about 9:35 a.m. School was dismissed early. Police and school district staff searched the building but found no suspicious objects. Authorities said a girl who

UNCLASSIFIED

attends the school was identified as a suspect and taken to the police department February 16.

Source: <http://www.chicagotribune.com/news/chi-ap-wi-bombthreatarrest,0,5567380.story>

(Ohio) State mailing exposes Social Security numbers. More than 8,000 state child-care providers in Ohio had their Social Security numbers accidentally exposed, WBNS 10 reported February 14. The providers received letters from Affiliated Computer Services, a subsidiary of Xerox. The company was hired by Ohio to manage a new automated system for paying and tracking child-care providers. "Xerox sent out a mailing to these providers and the mailing label on the envelope included their provider ID number," a spokesman with the Ohio Department of Job and Family Services said. "Now for a childcare center, that's not a big deal. It's a random six-digit number. For Type B providers, who offer childcare out of their own home, their provider number is their Social Security number." The numbers were printed on the outside of the envelopes where anyone could see them. State officials said identity theft protection would be provided to all affected workers. Source:

http://www.dispatch.com/live/content/local_news/stories/2011/02/15/social-security-numbers-exposed-wbns.html?sid=101

Official: 100 foreign agencies test US networks. More than 100 foreign intelligence agencies have tried to breach U.S. defense computer networks, largely to steal military plans and weapons systems designs, a top Pentagon official said February 15 at the RSA cybersecurity conference in San Francisco, California. The Deputy Defense Secretary said that while foreign governments and rogue states may try to launch more destructive attacks against military networks, most may stick to theft and spying because they are worried about a U.S. counterattack. The greater threat, he said, are terror groups such as al-Qaida, who are more difficult to deter. Terrorists have vowed to unleash cyberattacks, and over time may be able to either develop their own malicious computer threats or buy them on the black market. The Deputy Defense Secretary declined to specify how many of the 100 foreign intelligence agencies he said have tried attacks were successful in breaching U.S. government defenses, saying that would include classified information. He said the attacks involved espionage, such as seeking weapons design or diplomatic information, and didn't appear to be aimed at causing destruction of physical infrastructure. Source:

http://www.google.com/hostednews/ap/article/ALeqM5iGMAInxaJxFPsIHG0_RANRkiuEqQ?docId=f77c72e6081742d39398fd45bd36eadc

Federal official threats lead to few charges. Only a few dozen threats a year against federal officials result in prosecutions, often because it is impossible to identify a suspect, Justice Department (DOJ) officials said. A review of threat prosecutions by the Associated Press following the shootings of a Democratic U.S. Representative and a U.S. District Judge in January in Tucson, Arizona, showed it typically takes much more than posting warnings on obscure Internet sites to lead authorities to act. The people actually charged with threatening federal officials have taken the time to write, call, e-mail or appear in person to put their names behind their warnings. Each year, hundreds of threats make their way to the DOJ, according to government data compiled by Transactional Records Access Clearinghouse, a private, nonpartisan group based at Syracuse University in New York. Justice officials said many cases reach them before a suspect has been identified because investigators need subpoenas or other legal help in trying to trace a threat to its source. Often a suspect is never identified, so no prosecution is possible. Source:

<http://www.huffingtonpost.com/2011/02/14/federal-official-threats- n 822732.html>

UNCLASSIFIED

UNCLASSIFIED

(Tennessee) Shooting suspect on Tennessee university campus captured. A suspect is in custody about an hour after one person was shot February 14 on the campus of Middle Tennessee State University in Murfreesboro, Tennessee, a school spokesman said. Officials called off a lockdown, which had been in effect as SWAT teams and other law enforcement authorities converged on the campus, after the suspect was detained about 12:45 p.m., the university's media relations director said. A gun said to have been used in the incident has also been confiscated. Authorities were alerted at 11:51 a.m. about a shooting in a basic and applied science building located in a cluster of university structures. "From what I understand, there were two men who got into an argument over by some of our buildings," the media relations director said. "One shot the other in the hand, then took off." The victim, whose condition was not immediately known, was taken to a nearby medical facility. It was not confirmed whether those involved were students. Source:

<http://www.cnn.com/2011/CRIME/02/14/tennessee.school.shooting/index.html?hpt=T2>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Chinese mobile malware powers click-fraud scam. Malware writers are trying to infect Chinese users of Android smartphones with a Trojan that poses as a wallpaper for the smartphone's screen or other legitimate applications, such as the popular game RoboDefense. The mobile malware, dubbed Adrd or alternatively HongTouTou, has been seeded onto third-party mobile app stores in China. The official Android Market is not affected. If installed, the Trojan gathers the IMEI and IMSI numbers of compromised devices, uploading this information to a remote server, before generating counterfeit queries against particular search results. The malware specifically generated fraudulent clicks on the Baidu ad network, according to anti-virus firm AVG, which reckons the Trojan is the work of a group also producing malware targeting Symbian smartphone. Source:

http://www.theregister.co.uk/2011/02/17/android_trojan_click_fraud_scam/

Windows 0day could allow complete hijacking. Security researchers have warned of a new vulnerability afflicting older versions of Windows that could allow attackers to take complete control of machines running the operating systems. The flaw in "BrowserWriteErrorLogEntry()" function within the Windows mrxsmb(dot)sys driver "could be exploited by remote attackers or malicious users to cause a denial of service or take complete control of a vulnerable system," researchers from French security firm Vupen warned. The warning came after proof-of-concept code was posted February 14 to the Full-disclosure mailing list. Attacks are triggered by sending vulnerable machines malformed Browser Election requests that cause a heap overflow in the mrxsmb(dot)sys driver. The term "Browser" in this context does not refer to an application for browsing Web sites, but rather, to networking technology used by older versions of Windows. The malformed Browser Election requests contain an "overly long Server Name string," vulnerability tracking service Secunia said. Vupen, which rates the vulnerability as critical, has confirmed the bug in Windows Server 2003 SP2 and Windows XP SP3. Secunia rates it as moderately critical. Source:

http://www.theregister.co.uk/2011/02/16/windows_0day_vulnerability/

(dot)edu space filled with adult spam. Security researchers from GFI Software warned an increasingly large number of (dot)edu Web sites are being abused to push adult spam because of their poor security and lack of oversight. Searching for adult-oriented terms in the (dot)edu domain

UNCLASSIFIED

UNCLASSIFIED

space reveals entire pages of results, most of which are on discussion boards. “Most of this seems to have kicked in since around the 4th or 5th of February, and there doesn’t seem to be much in the way of spam control or preventative measures going on right now so please be careful if looking around your university forums, official or otherwise,” a security researcher at GFI said. It is not only forums that have been abused. Among search results users can also find what appear to be compromised Web sites. Most of them are installations of popular content management solutions that have been left unpatched for a long time. The same security holes can be leveraged to create malicious doorway pages that are part of malware distribution and black hat SEO attacks. A similar trend has also been observed for governmental Web sites, which are being abused by spammers and other cybercriminals not just in the United States, but internationally as well. Source:

<http://news.softpedia.com/news/EDU-Space-Filled-with-Adult-Spam-184302.shtml>

Complex Trojans and next generation malware is on the way. While e-mail users may have noticed a significant drop in spam in recent months, cybercriminals are gaining ground with creative new phishing methods and making exploit kits more robust, reveals the Security Labs Report from M86 Security. Findings include: third-party phishing is on the rise; e-mail spam is declining, though far from dead; there have been some notable bot-net take-downs and Spamit.com has closed; and exploit kits with virus scanners are becoming increasingly popular while social network attacks are increasing.

Source: <http://www.net-security.org/secworld.php?id=10594>

Fake scanned documents lead to Zeus infection. A new spam e-mail campaign is currently underway, and takes the form of a document scanned and sent by a Xerox WorkCentre Pro scanner. The attachment is a specially crafted PDF document, BitDefender warned, and it is able to exploit four Adobe Acrobat Reader vulnerabilities — all of which can be used by an attacker to remotely execute arbitrary code on a vulnerable system. In this case, the ultimate goal of the people behind this spam campaign is to spread the credentials-stealing Zeus trojan. Source: http://www.net-security.org/malware_news.php?id=1629

Security experts fear iframes on Facebook pages could spell trouble. Security experts fear the introduction of iframes for Facebook pages will open the door to abuse and will make the job of attackers on the social network much easier. Facebook announced February 10 Page administrators could start creating Page Tabs that load apps inside iframes instead of the more restrictive Facebook Markup Language. “While this is no doubt great news for legitimate developers, it will undoubtedly make life for those with malicious intent much easier too,” a senior security advisor at antivirus vendor Trend Micro said. “No more likejacking required, no more having to persuade users to install your app, if a criminal can make the bait sweet enough just to get you to visit the page, that is all they will require to start the chain that leads to your computer being compromised and used for criminal purposes,” he explained. Source: <http://news.softpedia.com/news/Security-Experts-Fear-IFrames-on-Facebook-Pages-Could-Spell-Trouble-183981.shtml>

NATIONAL MONUMENTS AND ICONS

(Tennessee) Man admits to setting fires in Cherokee National Forest. A Monroe County, Tennessee, man pleaded guilty February 15 in a U.S. district court to setting fires in the Cherokee National Forest. The 64-year-old man of Coker Creek admitted to setting two fires in the Ironsburg area in 2007.

UNCLASSIFIED

UNCLASSIFIED

According to court documents, he admitted he lit candles and left them at the base of a stump and a tree to start the fires. The fires damaged 26 acres. The U.S. Forest Service (USFS) suspected the man was a firebug for more than a decade but were unable to prove it. As part of his plea deal, the man has agreed to meet with USFS and share his fire-setting secrets. The agency hopes the information will help it detect arson in the future. The convict will be sentenced July 14. Source:

<http://www.wbir.com/news/article/157280/2/Man-admits-to-setting-fires-in-Cherokee-National-Forest>

(California) Marijuana farming in Calif. forest harms animals, pollutes water. The growing number of illegal marijuana farms in California's Los Padres National Forest is killing animals and polluting the land, officials said. A sergeant with the Ventura County Sheriff's Department narcotics bureau said not only do growers kill animals that get in the way of their gardens, but they also set up shop in natural habitats, poisoning water and land. "The fertilizers they use, Miracle-Gro and ammonium sulfate, they pour that right into soil ... I can't imagine drinking that water can be healthy for any animal," he said. The number of marijuana plants seized in the Ventura County portion of the Los Padres has increased by 10 percent since 2007, largely because of the presence of international drug cartels, according to the narcotics bureau. The amount of weapons seized also has risen — from one in 2007 to 31 in 2010. A warden with the California Department of Fish and Game, said the state's forests are ideal for marijuana cultivation, because of their isolation and year-round water supply, but the effects are clear. According to the Campaign Against Marijuana Planting, a statewide task force of nine state and federal agencies based in Sacramento, 4.3 million plants were seized across California in 2010. Source: <http://www.scrippsnews.com/node/59684>

POSTAL AND SHIPPING

Revamping inbound mail security. After an explosive printer cartridge was found last year en route to the United States in UPS and FedEx shipments, DHS tightened security for inbound international cargo and temporarily banned all shipments from Yemen. DHS and industry are now collaborating to establish "precautionary" security measures and improve the flow of parcels and packages. A DHS official who heads up mail issues at the office for international affairs said discussions at the highest levels focused on improving the situation for mail. He said DHS has been talking with the World Trade Organization, Universal Postal Union, PostEurop, and major postal operators including the U.S. Postal Service on how to improve the collection and handling of advanced notice data. The DHS official has been pushing for the adoption of internationally developed postal standards, and the recognition of certified companies and mail-handling buildings. A DHL Global Mail chief executive said the week of February 7 that security measures imposed by the Transportation Security Administration had "really put a lot of stress on things." Nevertheless, he said DHL was attempting to be pragmatic, working with DHS and TSA. "DHL is meeting all the requirements and exceeding them," he said. "We're still not out of it, but then there never will be 100 percent security." Source:

<http://homelandsecuritynewswire.com/revamping-inbound-mail-security>

(California) VA office in Palo Alto evacuated after letter found with suspicious substance. Authorities evacuated a 3-story office building at the Veterans Affairs (VA) Palo Alto Health Care System campus in Palo Alto, California, February 15 after an employee opened an envelope containing a suspicious substance and fell ill, a VA official said. The employee at Building 6 on the 3801 Miranda Avenue campus was going through mail when he opened the mysterious envelope, a

UNCLASSIFIED

UNCLASSIFIED

VA spokeswoman said. "In opening the envelope, he felt something gritty," she said. "It smelled musty." The alarmed man notified hospital staff, then became nauseous and vomited, the spokeswoman said. He was eventually treated in the emergency room on campus and released shortly afterward. The spokeswoman said initial reports indicated the substance was a white powder, but that proved to be false. Palo Alto police and the fire department's hazardous materials team responded, and the FBI and U.S. Postal Inspection Service are investigating. The FBI will analyze the envelope to determine the nature of the substance. Source:

http://www.mercurynews.com/peninsula/ci_17396584?source=most_email&click_check=1

PUBLIC HEALTH

FDA cites misuse of Medtronic drug pumps. Medtronic Inc. said February 16 it alerted physicians in January of potential danger from misuse of its implantable infusion pumps that led to eight deaths since 1996. The U.S. Food and Drug Administration on its Web site classified the issue as a Class I recall, which involves the potential of serious harm or death to patients. But Medtronic is not actually recalling its SynchroMed II and SynchroMed EL pumps as the problem is related to improper use rather than a defect in the devices. The infusion pumps, which are implanted into the abdomen, are used for constant delivery of drugs or fluids to patients. Problems arise when refills of the drugs are accidentally injected directly into the patients all at once rather than into the pump for gradual administration of the medication. Between May 1996 and September 2010, including an earlier version of the pumps that is no longer sold, there were reports of 8 deaths and 270 events requiring medical intervention, Medtronic said. Source: <http://www.reuters.com/article/2011/02/16/us-medtronic-idUSTRE71F7SZ20110216>

(California) Students need booster shots. By the start of the 2011-12 school year, all middle and high schools students in California will need to prove they have been immunized for pertussis. Whooping cough made a dramatic comeback in 2010 amidst a statewide outbreak of the highly infectious bacterial disease. Solano County and area school officials are gearing up to adhere to a new law that goes into effect July 1 requiring all incoming students grades 7 to 12 prove they received a booster shot. "This past year has been a pertussis epidemic but activity has been slowing. We're not getting the same number of cases we got in 2010," a Solano County deputy health officer said. Solano County saw 38 cases of whooping cough in 2010 and has had 2 so far this year, he said. California saw 8,627 cases in 2010 and about 311 this year. The last time there were more cases than in 2010 was in 1947. Source: http://www.thereporter.com/news/ci_17391367

US flu activity rises, shifts toward 2009 H1N1 strain. The nation's flu activity increased again for the fourth week in a row, and for the first time the number of specimens testing positive for the 2009 H1N1 virus topped the H3N2 strain, which for the past several weeks had dominated, the Centers for Disease Control and Prevention (CDC) said February 11. Most indicators have increased, including doctor's visits for flu-like illness. That marker rose to 4.6 percent, up from 4 percent the week before, which puts the level well above the national baseline of 2.5 percent. The only one of the CDC's 10 regions where doctor's visits for flu were still below the regional baseline is the one that includes Arizona, California, Guam, Hawaii, and Nevada. Flu also expanded its reach and intensity the week of February 7, with 37 states now reporting widespread activity, 7 more than the previous week. Eleven pediatric flu deaths were reported the week of February 7, raising the total for the season to 30 from

UNCLASSIFIED

UNCLASSIFIED

18 states. Of the newly reported fatalities, 4 were linked to influenza B, 2 to 2009 H1N1, 1 to H3N2, and 4 to undetermined influenza A subtypes. Source:

<http://www.cidrap.umn.edu/cidrap/content/influenza/swineflu/news/feb1111flu-jw.html>

(Michigan) Hospital employee arrested on charges of threats of terrorism. An employee of the West Branch Regional Medical Center in West Branch, Michigan was arrested after allegedly making threats of violence at the hospital, according to a press release from the West Branch City Police Department. According to the release, the 32-year-old Gladwin resident and employee at the medical center was allegedly overheard making several threats of violence by multiple witnesses January 28. A warrant was issued for the man's arrest by an Ogemaw County prosecutor for threats of terrorism. He was arrested at his residence February 10, and was housed in the Ogemaw County Jail. His arraignment began February 11, and was scheduled to conclude February 15. Source:

http://www.ogemawherald.com/detail/88029.html?content_source=&category_id=1&search_filter=&list_type=&order_by=&order_sort=&content_class=1&sub_type=&town_id=7

South African appears in court on terror charges. A South African businessman accused of threatening to unleash biological weapons on Great Britain and the United States may have been driven by concern over the plight of white farmers in neighboring Zimbabwe, a spokesman for the prosecution said February 14. The suspect did not have the means to carry out his threats to spread foot and mouth disease. The 64-year-old man, who owns an engineering firm outside Johannesburg, South Africa, appeared in a Johannesburg court after his arrest February 12 on terror charges. He threatened in letters and e-mails sent to the British government to spread the disease in Britain and the United States unless he was given \$4 million. "We have the expertise and resources to do this very effectively and will be able to devastate the industry in the U.K. which will cost billions to the economy," he wrote in an e-mail to the British government. "We will devastate your farms and then we will then take the problem to your coconspirator the USA." South African police said a 6-month terror investigation by South African, British, and U.S. officials culminated with his arrest. U.S. and British officials confirmed they had worked closely with the South Africans. Police charged the man with terrorist activity and money laundering. Source:

http://news.yahoo.com/s/ap/20110214/ap_on_re_af/af_south_africa_terror_arrest

TRANSPORTATION

United: Operations back to normal as 757 inspection continues. United Airlines said it canceled 15 flights late February 15, after grounding its fleet of 96 Boeing 757s over safety issues, but expected to resume normal operations February 16. The carrier voluntarily halted 757 takeoffs after it discovered it hadn't completed safety checks on a critical equipment upgrade required by federal aviation regulators. As of the morning of February 16, United hadn't completed inspecting all 757s, but expected to complete them "shortly," a spokeswoman said United uses the planes mostly on long-range flights. The problem occurred on the 757's air data computer, which measures air pressure and other atmospheric conditions to determine speed and altitude. On June 22, 2004, the Federal Aviation Administration (FAA) ordered the computers be replaced and that mechanics perform a check to ensure they were working properly. United hadn't performed the required check after replacing the units. The airline said it was not aware of any problems or incidents caused by the computers. Each 757 has two of the computers so they can check each other's accuracy, as well as a

UNCLASSIFIED

UNCLASSIFIED

standby system in case of emergency, according to Boeing documentation. The FAA issued an emergency order requiring the computers be replaced because of a flaw that could cause pilots to erroneously believe they were flying too fast or too slow. The agency was unaware of the issue until it was notified February 15 by United, an FAA spokeswoman said. Although rare, erroneous speed readings have led to several fatal crashes, including two in 1996 on 757s, a USA TODAY report found.

Source: <http://travel.usatoday.com/flights/post/2011/02/united-operations-back-to-normal-as-757-inspection-continues/143332/1>

(Ohio) 5 planes destroyed by arson at Brookville Airpark. Fire officials determined arson was the cause of a February 14 fire that destroyed two hangars and five airplanes at the Brookville Air Park in Montgomery County, Ohio. Investigators with the division of state fire marshal said they “found evidence indicating the fires were intentional set,” a spokesman with the Ohio Department of Commerce said. Firefighters were called to 9386 W. National Road at 2:21 a.m. The hangars are located 580 feet apart, and the investigation showed both were set on fire. The east side hangar contained three single-engine aircrafts, and the west side hangar had two aircrafts (one single-engine and one twin-engine) that were destroyed. Fire officials said one of the hangars was also a repair shop that had some propane tanks inside. The Brookville fire chief said the investigation was being handled by the state fire marshal, Brookville Fire Department, Clay Township Police, and the Federal Aviation Administration. Source: <http://www.daytondailynews.com/news/dayton-news/5-planes-destroyed-by-arson-at-brookville-airpark-1081092.html>

WATER AND DAMS

Nothing Significant to Report

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7): 866-885-8295(IN ND ONLY)**; Email: ndslic@nd.gov ; Fax: 701-328-8175
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED