



**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

**Informants can now text crime tips in Cass County.** Cass County, North Dakota officials have developed a system they say will make it easier for the public to report crime tips. The Cass County Sheriff's Office recently implemented a program that allows cell phone users in the county to provide anonymous tips via text messaging or the Web. The service was built specifically to allow text messaging informants to remain anonymous by encrypting the text messages and routing them through several secure servers, which protects the personal details of the informant. The program also allows police to respond by text message to the originating cell phone without knowing the identity of the individual who left the tip, according to a news release. This secure application allows the tipster and the investigator to have two-way dialogue without jeopardizing the identity of the person. Source: <http://www.southbendtribune.com/article/20101201/News01/101209958/-1/googleNews>

**Railroad disputes accident findings.** The Federal Railroad Administration (FRA) said a saturated road bed, weakened by the failure of the railroad track's drainage system, was the probable cause of a March 25 derailment that killed a railroad conductor and injured an engineer south of Washburn, North Dakota. Officials from the Dakota Missouri Valley and Western (DMVW) Railroad dispute the FRA findings, saying the accident was caused by an unknown underground spring that eroded the bank below the track. An FRA spokesman sent an e-mail November 30 saying the agency's attorneys will review the incident report and determine if fines are warranted. The conductor died after two DMVW railroad engines derailed on an embankment that gave way just above Turtle Creek, feeding the Missouri River. No hazardous materials were loaded on the train. The FRA report said the locomotives leaked about 2,000 gallons of diesel fuel, but the fuel was contained and did not enter Turtle Creek or the Missouri River behind it. Tainted soil was removed and properly disposed of, according to federal and state guidelines. Source: [http://www.bismarcktribune.com/news/local/article\\_355cf882-fcd3-11df-8296-001cc4c03286.html](http://www.bismarcktribune.com/news/local/article_355cf882-fcd3-11df-8296-001cc4c03286.html)

## REGIONAL

**(Minnesota) Vehicle hits power pole, cuts out electricity in St. Cloud.** Thousands of Xcel Energy consumers were temporarily without power November 26-27 because of a vehicle crashing into a power pole, according to a company spokeswoman. At 11:13 p.m. November 26, a vehicle crashed into a power pole, causing loss of power to 2,750 costumers in St. Cloud, Minnesota, an Xcel spokeswoman said. Power was restored by 12:19 p.m. November 27. The spokeswoman said that an Xcel crew's attempt to replace the pole at 5:56 a.m. led to a second power outage for 5,000 Xcel customers until 7:32 a.m., when power was once again restored. Source: <http://www.sctimes.com/article/20101128/NEWS01/111280022/1009>

**(South Dakota) Study finds high levels of bacteria in area rivers.** A two-year study recently revealed both the Big Sioux River and other streams from Dell Rapids, South Dakota to Brandon, South Dakota

## UNCLASSIFIED

are listed by the South Dakota Department of Environmental and Natural Resources as having impaired water quality. This means there is excess sediment and bacteria in the water. The results mean decades of work to bring the Big Sioux and other bodies of water up to the U.S. Environmental Protection Agency's (EPA) water quality standards. The study only involved bodies of water designated for recreational use and did not affect drinking water. The purpose of the study was to figure out where the excess bacteria is coming from. Once the Total Daily Maximum Load is approved, the area's agricultural community is eligible for federal funding to help improve water quality. Source: <http://www.ksfy.com/Global/story.asp?S=13600749>

**(Wyoming) Herd tests positive for brucellosis.** A second cattle herd in Park County, Wyoming, was confirmed to test positive for brucellosis. A state veterinarian said this case is not connected to another herd that tested positive earlier this month, and it most likely caught the disease from free roaming elk. "The culture we took is the same that's showing in the elk," he said. This new case still will not affect the brucellosis-free status of the state, he said. Two of 12 cattle within Wyoming's Designated Surveillance Area, where cattle have to be tested before changing ownership, showed positive for the bacterial disease. Source:

[http://www.codyenterprise.com/news/local/article\\_8f847a76-fc09-11df-9a90-001cc4c002e0.html](http://www.codyenterprise.com/news/local/article_8f847a76-fc09-11df-9a90-001cc4c002e0.html)

## **NATIONAL**

**(New York) Snow strands hundreds of drivers in western NY.** Hundreds of motorists were stranded on a western New York highway December 2 after an accident caused a backup and the idling cars became stuck overnight in heavy snow. A 10-mile section of Interstate 90 was closed in both directions in Buffalo's eastern suburbs. The highway was closed shortly before 3 a.m. December 2 after vehicles backed up behind a truck accident became buried in blowing snow. The truck jackknifed around 8 p.m. December 1 and has been removed, but crews were still working the morning of December 2 to free the stranded vehicles. The lake-effect storm that began December 1 dumped up to 23 inches on the Buffalo area. Power remains out for about 10,000 utility customers in eastern New York. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5ioLVICPDcC78iF5xXmQvXI0TGrkA?docId=ffc b54f24d9044ddaf747f2d1216c59e>

**(California) Cal gov declares state of emergency in SD County.** The governor of California declared a state of emergency December 1 in San Diego County following the discovery of what police called a "virtual bomb factory" in an Escondido-area home. Under the declaration, the California Emergency Management Agency will coordinate the efforts of all state agencies and provide assistance to San Diego County to remove the hazardous materials. The declaration came a day after authorities said that they plan to burn down the home the week of December 6 because it is the only way to eliminate the danger from the massive stockpile of unstable, highly explosive materials — including a variety of powders, sulfuric acid, nitric acid, and hydrochloric acid — found inside. Earlier December 1, a search warrant was released that said a resident of the home who possessed the explosives told authorities he robbed three banks and tried to rob a fourth. The chemicals found in the house are the same type as those used by suicide bombers, insurgents in Iraq and Afghanistan, and in the 2001 airliner shoe-bombing attempt as well as in last month's airplane cargo bombs, authorities said.

Source: <http://www.foxnews.com/us/2010/12/01/warrant-calif-bomb-suspect-says-robbed-banks/>

UNCLASSIFIED

## UNCLASSIFIED

**US officials warn warehouse owners near border to watch for tunnelers.** U.S. federal authorities are going door to door in San Diego, California, warning warehouse owners near the U.S.-Mexico border to watch out for tunnelers. Authorities with the Federal Tunnel Task Force are passing out fliers to warehouse owners in Otay Mesa — the industrial area just a few hundred feet from the border fence. An Immigration and Customs Enforcement spokeswoman said it is an area where authorities have seen a growing number of tunnels inside warehouses in the last few years. Authorities have unearthed two sophisticated drug smuggling tunnels in Otay Mesa in the last month. Both had rail systems, one with a motorized cart, to move bales of drugs from Tijuana to San Diego. The flier federal agents are passing out asks people to report subterranean noises, unexplained vibrations, and the odor of marijuana. It also asks warehouse owners to keep an eye out for renters who pay in cash, are unusually withdrawn, or keep unusual business hours. Source:

<http://www.kpbs.org/news/2010/nov/29/us-officials-warn-warehouse-owners-near-border-wat/>

**(California) Officials pull out of CA bomb factory, cite danger.** Explosives experts have pulled out of a San Diego County, California home described as a virtual bomb-making factory because it is too dangerous to remove some of the materials discovered inside the rental property. Operations at the Escondido home were suspended November 24 until local, state and federal explosives experts can make plans to re-enter it and remove blasting caps and dangerous chemicals, the county sheriff's department said in a statement. Prosecutors have said the materials make up the largest amount of certain homemade explosives in one location in U.S. history. Explosives were discovered in his rented home after a gardener was injured earlier in November in a blast that occurred when he stepped on explosive powder in the backyard, authorities said. Investigators said they found 13 unfinished shrapnel grenades, and at least 9 pounds of dangerous materials in and around the home. Authorities said it is unclear what the suspect may have planned to do with the materials. The same types of chemicals have been used by suicide bombers and insurgents in Iraq and Afghanistan. They included Pentaerythritol tetranitrate, or PETN. The other chemicals were highly unstable Hexamethylene triperoxide diamine, or HMTD, and Erythritol tetranitrate, or ETN, authorities said. Investigators said they also found gallons of hydrochloric, nitric and sulfuric acid, and 50 pounds of the toxic chemical hexamine. Source: [http://news.yahoo.com/s/ap/20101126/ap\\_on\\_re\\_us/us\\_backyard\\_explosion](http://news.yahoo.com/s/ap/20101126/ap_on_re_us/us_backyard_explosion)

## **INTERNATIONAL**

**International fire aid reaches Israel.** Firefighting aircraft from Bulgaria, Cyprus, Greece, and Britain arrived in Israel to help battle the massive forest fire that has claimed 41 lives, police said. The firefighting planes went into operation December 3 and began dousing the flames that have already destroyed thousands of acres in the Carmel Forest area, Israel rescue officials told Israel Radio. France, Romania, Egypt, Jordan, Turkey, Russia, and the United States all pledged to send aircraft, firefighting teams, and equipment to help extinguish the blaze that also threatened the outskirts of Israel's third largest city, Haifa. The number of fatalities rose to 41 December 3, Israel police said, after 36 Israel Prison Service cadets were killed along with two officers and a civilian when the bus they rode in was engulfed in flames December 2. Source: [http://www.upi.com/Top\\_News/World-News/2010/12/03/International-fire-aid-reaches-Israel/UPI-70311291373487/](http://www.upi.com/Top_News/World-News/2010/12/03/International-fire-aid-reaches-Israel/UPI-70311291373487/)

**US airport security program to launch in Yemen.** A U.S.-style airport security program will soon be set up in Yemen, where an Al-Qaeda affiliate has engineered a string of failed international airline attacks, U.S. officials said. "We have a program that will be starting up in the very near future, an 18-

UNCLASSIFIED

## UNCLASSIFIED

month program with Yemen,” an official with the U.S. Transportation Security Administration told a Senate hearing on international airline safety. Yemen-based Al-Qaeda in the Arabian Peninsula has claimed it was behind a foiled air cargo bomb plot in October, in which printer toner cartridges that had been rigged as bombs were shipped out of Sanaa. Source:

<http://www.google.com/hostednews/afp/article/ALeqM5hpA1839r1T5ZpKSJrVVqWuqvGoNA?docId=CNG.f9a0b4d03dfba10ea4d940df1f67012d.b71>

**Oz bank meltdown due to file corruption.** The 5-day mainframe bank system meltdown at the National Bank of Australia (NAB) was due to a corrupted file on an IBM mainframe system that was being upgraded. Staff attempted the upgrade November 25, but it failed to complete. It was reversed and that was when, it appears, ongoing payment processing data in a file was corrupted. It caused payments to stop or to be recorded incorrectly, with some customer accounts having multiple incorrect debits applied. Money transfers to other banks as well as the NAB’s own customers were affected. Private and business customers were prevented from accessing their accounts at ATMs and electronic funds transfer payments stopped. Customers had to attend branches in person to get cash, and the bank hurriedly opened some branches November 28 to cope with the rush. A payment processing backlog built up. Some customers had interest applied to illusory debts in their accounts, and the bank’s support staff had the massive job of rolling everything back to a known good point, and then reapplying transactions in strict time to get everything back up to date. The bank has promised that disadvantaged customers will have their accounts put right. Source:

[http://www.theregister.co.uk/2010/11/29/nab\\_mainframe\\_cockup/](http://www.theregister.co.uk/2010/11/29/nab_mainframe_cockup/)

**Somali pirates hijack Malaysian ship, 23 crew.** Somali pirates have hijacked a Malaysian-flagged container ship in the Indian Ocean. Multiple sources said November 30 that pirates seized the MV Albedo west of the Maldives islands November 26. The ship was en route from the United Arab Emirates to Kenya. The European Union’s anti-piracy force said the Albedo has a crew of 23 from Pakistan, Bangladesh, Sri Lanka, and Iran. Somali pirates are now reported to be holding at least 22 vessels with more than 500 hostages. Pirates have continued to hijack ships despite naval patrols by the European Union, the North Atlantic Treaty Organization, and countries such as Russia and China. Source: <http://www.voanews.com/english/news/africa/Somali-Pirates-Hijack-Malaysian-Ship-23-Crew-111034399.html>

**Puerto Rican breach affects 400,000.** About 400,000 Puerto Ricans enrolled in the government’s health insurance plan for the impoverished have potentially been affected by a breach incident involving unauthorized access to an Internet database. Triple-S Management Corp., a holding company that runs Blue Cross and Blue Shield plans and serves as a government contractor, said in a recent 10-Q securities filing that a competitor informed it that “certain of our competitor’s employees” accessed the database without permission September 9-15. The database included information pertaining to individuals previously insured under the government health plan that was managed by a Triple-S subsidiary, as well as information about the independent practice associations that provided services to those individuals. “The database intrusion may have potentially compromised protected health information of approximately 398,000 beneficiaries,” according to the 10-Q filing. The company said its investigation also revealed protected health data of about 5,500 government health insurance plan beneficiaries and 2,500 Medicare beneficiaries, plus certain independent practice association data, was inappropriately accessed through multiple intrusions into the database from October 2008 to August 2010. The information accessed did not include Social

UNCLASSIFIED

Security numbers, the company said. Source:

[http://www.healthcareinfosecurity.com/articles.php?art\\_id=3129](http://www.healthcareinfosecurity.com/articles.php?art_id=3129)

## **BANKING AND FINANCE INDUSTRY**

**FBI warns consumers about bogus lottery notifications.** The FBI's cyber crime center IC3 continues to receive reports of consumers receiving letters and e-mails declaring them as winners of sweepstakes and lottery schemes. These schemes employ counterfeit checks with legitimate-looking logos of financial institutions to fool victims into sending money to the fraudsters. Crooks tell victims they won a sweepstakes or lottery, but to receive a lump sum payout, they must pay taxes and processing fees upfront. The e-mail recipients are instructed to start the process by calling a phone number. The letter says the victim may choose to take an advance on the winnings to make the required upfront payment. The letter also includes a check in the amount of the alleged taxes and fees, along with processing instructions. Ultimately, victims believe they are using the advance to make the required upfront payment. The victim deposits the check into their own bank, which credits the account for the amount of the check before the check clears. The victim then immediately withdraws the money and wires it to the fraudsters. Afterward, the check turns out to be bogus and the bank pulls the respective funds from the victim's account, leaving him or her liable for the amount of the counterfeit check plus any additional fees that may have occurred. Source:

<http://www.thenewnewinternet.com/2010/12/01/fbi-warns-consumers-about-bogus-lottery-notifications/>

**Internet gaming and e-commerce phishing assaults explode.** Internet Identity (IID) services and technology provider recently published its Phishing Trends Report that found global phishing attacks based on mimicking gaming and e-commerce Web sites rose considerably from one year to another during July-September 2010 i.e. Q3-2010. The report said cases in which cyber-criminals impersonated e-commerce Web sites, other than eBay, to capture sensitive information from unwitting users, rose 317 percent during Q3-2010 in contrast with Q3-2009. Similarly, phishing assaults mimicking online games rose 347 percent during Q3-2010 in contrast with Q3-2009. IID thinks this trend will continue in Q4-2010, given past history. For instance, over Q3-Q4 2009, phishing attacks on e-commerce Web sites, other than eBay, rose 86 percent. IID states that in spite of the growing number of gaming and e-commerce Webs ite phishing attacks, these sectors are subject to just 7 percent each of all spoofed assaults. The maximum number of phishing assaults (79 percent) happens within the money-transfer and banking sectors; 4 percent occur through social networks and e-mail; and 3 percent from operations within "other" sectors. The president and CTO of IID said conventional cyber-criminals exploited ongoing events, leading to a rise in phishing assaults spoofing e-commerce Web sites on the run up and at the time of the vacation period when shopping was the highest. He further said that as people globally became active participants during the excessive Internet shopping season, there could be rises in e-commerce assaults worldwide. Source:

<http://www.spamfighter.com/News-15452-Internet-Gaming-and-E-Commerce-Phishing-Assaults-Explode.htm>

**WikiLeaks will unveil major bank scandal.** First WikiLeaks exposed government secrets. Next up: The private sector, starting with one major American bank. In an exclusive interview earlier in November, the WikiLeaks founder told Forbes that his whistleblower site will release tens of thousands of documents from a major U.S. financial firm in early 2011. The WikiLeaks founder would not say

## UNCLASSIFIED

exactly what date, what bank, or what documents, but he compared the coming release to the e-mails that emerged in the Enron trial, a comprehensive look at a corporation's bad behavior. "It will give a true and representative insight into how banks behave at the executive level in a way that will stimulate investigations and reforms, I presume," he told the Forbes reporter. Source:

<http://blogs.forbes.com/andygreenberg/2010/11/29/exclusive-wikileaks-will-unveil-major-bank-scandal/?boxes=Homepagechannels>

**First arrest in wide insider-trading probe.** The FBI has made the first arrest in a sweeping insider-trading investigation targeting hedge funds and others. One male suspect was arrested November 24 at his Somerset, New Jersey, home and charged with conspiracy to commit securities fraud and conspiracy to commit wire fraud. According to prosecutors, while at Primary Global Research, the suspect provided confidential tips about Atheros Communications, Broadcom Corp., and Sierra Wireless Inc. to a hedge fund manager. The suspect's arrest provides the first concrete link between the current insider-trading investigation, which has seen three hedge funds raided and dozens of others served with subpoenas, and the Galleon Group insider-trading case. The former hedge fund manager, who ran Spherix Capital, is a cooperating witness in the Galleon case. Source:

<http://www.finalalternatives.com/node/14698>

## CHEMICAL AND HAZARDOUS MATERIALS SECTOR

**Stuxnet researchers cautious about Iran's admission of centrifuge issues.** Although Iran apparently confirmed November 29 that the Stuxnet worm disrupted the country's uranium enrichment efforts, one of the researchers who has dug deepest into the malware was not ready to call it a done deal. "If that information is accurate, then, yes, it's very interesting," said the manager of operations on Symantec's security response team, in an interview November 29. If Stuxnet did affect centrifuges used to enrich uranium at Iran's nuclear sites, the official continued — again stressing the word "if" — that would mean that Symantec's latest analysis of the worm was on the mark. "But we'd like to get firm confirmation that Stuxnet was definitely used to disrupt centrifuges," he said. But that proof may never come, despite announcement November 29 by the Iranian President that enemies of his country had "succeeded in creating problems for a limited number of our centrifuges with the software they had installed." Iran's story on Stuxnet has changed in the past several months, and it is possible that the Iranian President's admission was a smokescreen for more prosaic problems.

Source:

[http://www.computerworld.com/s/article/9198579/Stuxnet\\_researchers\\_cautious\\_about\\_Iran\\_s\\_admission\\_of\\_centrifuge\\_issues](http://www.computerworld.com/s/article/9198579/Stuxnet_researchers_cautious_about_Iran_s_admission_of_centrifuge_issues)

**EPA screens 1,000 chemicals using ToxCast.** The U.S. Environmental Protection Agency's (EPA) ToxCast screening program has entered a new phase, screening 1,000 chemicals for potential toxicity to people and the environment. ToxCast is designed to determine how chemical exposures impact the human body and how the chemicals most likely lead to health effects. When fully implemented, ToxCast will be able to screen thousands of chemicals in fast, cost-effective tests that provide people with relevant information. During the first phase ToxCast tested about 300 chemicals, primarily pesticides, in more than 500 fast, automated tests or assays. The assays use human and animal cells and proteins to screen chemicals. Another 700 chemicals are now being screened in ToxCast's second phase. The chemicals being tested are found in industrial and consumer products, food additives and drugs that never made it to the market. ToxCast is reducing EPA's reliance on slow and expensive

UNCLASSIFIED

## UNCLASSIFIED

animal toxicity tests, enabling the agency to screen chemicals more quickly and to predict and identify potential health risks. EPA scientists have compared the first phase of ToxCast data to the vast number of animal studies available in EPA databases. Source:

<http://yosemite.epa.gov/opa/admpress.nsf/0/73EC2518E34BC93D852577EB0060DD7C>

**(Nebraska) NPPD gets 20-year license to operate nuke plant.** Nebraska Public Power District (NPPD) has been given federal permission to continue operation of Cooper Nuclear Station near Brownville in southeast Nebraska. The Lincoln Journal Star said the utility CEO signed papers for a 20-year license extension November 29. NPPD said the plant can generate as much as 810 megawatts of electricity. It began commercial operation in 1972. Source: <http://www.nebraska.tv/Global/story.asp?S=13586636>

## **COMMERCIAL FACILITIES**

**(Pennsylvania) Arrest made in North Side copper thefts.** Pittsburgh, Pennsylvania police arrested a homeless man November 30 and charged him with stealing copper wire from Heinz Field stadium property, and they suspect he and another man took nearly \$30,000 worth of the material in November. Security officers at Heinz Field saw a man pushing an empty shopping cart about 2 a.m. November 29 outside a white tent near the North Shore stadium's Gate A. The tent — nearly 100 feet long — stores copper and construction materials for the nearby Stage AE amphitheater set to open December 4, police said. Someone broke into the tent at least five times in the past month, police said, and security officers monitor video cameras in the area. The suspect went out of view of the cameras and moments later reappeared pushing the cart "loaded with wire," according to a police affidavit. Heinz Field primarily serves as the home to the National Football League's Pittsburgh Steelers, and the University of Pittsburgh. Source:

[http://www.pittsburghlive.com/x/pittsburghtrib/news/s\\_711617.html](http://www.pittsburghlive.com/x/pittsburghtrib/news/s_711617.html)

**(Oregon) Oregon resident arrested in plot to bomb Christmas tree lighting ceremony in Portland.** A 19-year-old naturalized U.S. citizen from Somalia and resident of Corvallis, Oregon, has been arrested on charges of attempting to use a weapon of mass destruction (explosives) in connection with a plot to detonate a vehicle bomb at an annual Christmas tree lighting ceremony November 26 in Portland, Oregon, the Justice Department announced. According to a criminal complaint signed in the District of Oregon, the man was arrested by the FBI and Portland Police Bureau November 26 after he attempted to detonate what he believed to be an explosives-laden van that was parked near the tree lighting ceremony in Portland's Pioneer Courthouse Square. The arrest was the culmination of a long-term undercover operation, during which the man had been monitored closely for months as his alleged bomb plot developed. The device was in fact inert; and the public was never in danger from the device. The man is expected to make his initial appearance in federal court in Portland November 29. He faces a maximum statutory sentence of life in prison and a \$250,000 fine if convicted of the charge of attempting to use a weapon of mass destruction. Source:

<http://portland.fbi.gov/dojpressrel/pressrel10/pd112610.htm>

**(Michigan) Police: 2 men shot inside suburban Detroit mall.** A dispute between two rival groups of teenagers escalated into gunfire November 27 when members of one of the groups opened fire inside a shopping mall, critically injuring one teenager and a clothing store worker as holiday shoppers dashed for cover, police said. The shooting happened around 6 p.m. at Eastland Mall, east of Detroit, Michigan. The mall was closed for the night as police searched for suspects, said the

UNCLASSIFIED

## UNCLASSIFIED

Harper Woods deputy police chief. The 18-year-old victim, a member of the rival group, was struck in the chest, and a stray bullet hit the leg of the worker, in his mid-30s, who was standing outside the clothing store, he said. Both were taken to St. Johns Hospital in Detroit. They were listed in critical condition but were expected to survive. The deputy chief said the shooting caused panicked shoppers to run for cover or exits as chaos unfolded inside the mall, which has more than 100 stores and restaurants, according to its Web site. Source:

[http://news.yahoo.com/s/ap/20101128/ap\\_on\\_re\\_us/us\\_detroit\\_mall\\_shooting](http://news.yahoo.com/s/ap/20101128/ap_on_re_us/us_detroit_mall_shooting)

**(Oregon) Arson attack on Corvallis Islamic center.** FBI agents are investigating an arson-caused fire at the Salman AlFarisi Islamic Center in Corvallis, Oregon. It was reported at 2:15 a.m. November 28 by a police officer who was patrolling the area. Firefighters responded quickly and extinguished it within 10 minutes. There was considerable fire and smoke damage to the office of the Islamic Center, which was the one frequented by the man accused of trying to explode a bomb in Portland's Pioneer Courthouse Square November 26. Two rooms adjacent to the office also suffered some light smoke damage. There was no damage to any worship area, the imam said. The mosque did not show visible external damage. The center is located at 610 NW Kings Boulevard near the Oregon State University campus. The FBI is offering a reward of up to \$10,000 for information leading to the identification, arrest, and conviction of the person or people responsible. Source:

[http://www.koinlocal6.com/content/news/topstories/story/Arson-attack-on-Corvallis-Islamic-Center/WcV9GbFjFEK484l8RXMU\\_w.csp](http://www.koinlocal6.com/content/news/topstories/story/Arson-attack-on-Corvallis-Islamic-Center/WcV9GbFjFEK484l8RXMU_w.csp)

**(Maryland) Three injured in early morning shooting near Fort Meade.** A man was shot three times on the parking lot of an Odenton, Maryland, bar, and two patrons were struck by stray bullets just outside the establishment November 27, Anne Arundel County police said. Officers found a man with bullet wounds to his head, back, and abdomen, lying on a parking lot behind My Place Bar & Lounge in the 1600 block of Annapolis Road shortly before 2 a.m., police said. Two other men were hit by stray bullets as they entered the bar, located in a strip of clubs and restaurants nicknamed "Boomtown," across from the Fort Meade military base, police said. Police said they found a 23-year-old suspect, of Halethorpe, crouched behind a fence of a nearby KFC restaurant. The suspect was charged with three counts of attempted first-degree murder along with other charges and held at the Anne Arundel Detention Center. Source: <http://www.baltimoresun.com/news/maryland/anne-arundel/bs-md-ar-odenton-bar-shooting-20101127,0,2567303.story>

## **COMMUNICATIONS SECTOR**

**(Florida) 3rd copper theft reported from a Molino tower.** For the second time in just over 2 months, copper wiring was stripped from a county-owned radio tower in Molino, Florida. The theft was discovered December 2 at the communications tower, which is located behind the Escambia County Health Department on Highway 29. Each time, the thief removed copper wiring that is part of the tower's grounding equipment. Radio communications using the tower were not interrupted. In October, a technician for CES Team One Communications, the company that maintains the radio tower for Escambia County, discovered items worth about \$3,450 missing from the tower. That theft occurred sometime between September 1 and October 11. On November 22, technicians discovered hundreds of dollars in copper grounding wire missing from the privately owned communications tower adjacent to the Molino Ballpark on Crabtree Church Road. The wiring was part of that tower's electrical grounding system. There were no reports that any of the services on the tower were

UNCLASSIFIED

## UNCLASSIFIED

disrupted. At least one cellular telephone company serves the Molino area from the tower. Source: <http://www.northescambia.com/?p=37150>

**(Georgia) AT&T goes after copper wire thieves.** Copper thieves targeting Atlanta, Georgia are now being targeted themselves by AT&T, which is offering \$3,000 for information leading to arrests. The Atlanta Journal-Constitution (AJC) reported that in one recent 3-day stretch, nearly 7,000 customers and two schools lost land line phone service. A cell phone tower also was temporarily knocked out. AT&T saw 11 thefts in 1 week in one location, including 8 in one morning. Damage to telephone lines exceeded \$500 in each case. Georgia law makes that a felony, punishable by jail time and fines, the AJC report stated. Source: <http://www.networkworld.com/community/node/68972>

**T-Mobile G2 hardware security hacked completely!** Even though T-Mobile took a lot of precautionary measures to make sure that the G2 phone would not be able to be rooted, the hardware is now fully unlocked. This is more than just simply rooting and putting ROMs on, the hardware is now completely open for development. Unlocking the phone is a very complicated process done by some pro developers who know exactly what they are doing, but they are certain to post a step by step guide on how normal android users can do it. Source: <http://androidcommunity.com/t-mobile-g2-hardware-security-hacked-completely-20101130/>

**P2P-based alternative to DNS hopes to challenge ICANN.** A group led by the former Pirate Bay spokesman is forming to develop a peer-to-peer-based alternative to today's ICANN-controlled DNS system, according to a blog posted November 30. He went public with the project, which also includes an alternative root server, on his Twitter account. The first step is a new root server, and the second step will be a new DNS system, he said. The P2P DNS project is aimed at keeping the Internet uncensored, the blog post said. The underlying infrastructure will be based on BitTorrent technology. To improve security, the data and the transmission will be signed, he said. Developing a system that can compete with DNS will be not be easy. One of the main challenges will be to offer the same robustness, said an IT security advisor at Swedish consultant Kirei. The P2P DNS Project could succeed in attracting users in file-sharing circles, but will have a hard time getting other users on board. The project could also come to realize the security advisor's greatest fear, which is DNS will be split into different parts. Source: [http://www.computerworld.com/s/article/9198638/P2P\\_based\\_alternative\\_to\\_DNS\\_hopes\\_to\\_challenge\\_ICANN](http://www.computerworld.com/s/article/9198638/P2P_based_alternative_to_DNS_hopes_to_challenge_ICANN)

**(California) AT&T blames vandals for outages.** AT&T is confirming reports of vandalism at several East and South Bay, California locations that cut off service to some customers November 25-26. A spokesperson said lines were cut in 15 locations causing a loss of both phone and Internet service to customers in Walnut Creek, Orinda, and Morgan Hill. The outages began November 25. AT&T crews worked through the night to repair those lines and expected all customers to be back up and running by November 26. They would not say how many customers were affected. Source: [http://abclocal.go.com/kgo/story?section=news/local/east\\_bay&id=7811914](http://abclocal.go.com/kgo/story?section=news/local/east_bay&id=7811914)

**FBI warns of mobile cyber threats.** People should be wary of criminal efforts targeting their cell phones, the FBI is warning. The agency's Internet Crime Complaint Center (IC3) said that creative criminals will be using scams called "smishing" or "vishing" to steal people's personal information, such as bank account numbers, personal identification number (PIN) codes, or credit card numbers.

UNCLASSIFIED

## UNCLASSIFIED

Smishing is a combination of SMS texting and the common online practice of phishing, which uses e-mails to direct people to Web sites where they are asked to give up personal information. In a smishing scam, people receive a text message on their phone telling them there is a problem with their bank account. The message will contain a phone number to call or a Web site to log into. To pull off these crimes, people set up an automated dialing system to text or call mobile phone subscribers in a particular region or area code. They also steal phone numbers from banks and credit companies and target people on these lists, according to the FBI. If a person follows through and follows directions, it is likely there is a criminal on the other end stealing personal information. Vishing is similar to smishing except instead of an SMS, a person will receive a voicemail giving them the same information. People who fall victim to mobile device scams could be in danger even if they stop short of giving up the information requested, the FBI warned. If they only log onto the fake Web site via their mobile device, they could end up downloading malicious software giving criminals access to anything on their phone, the agency said. Source:

[http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=228400096&cid=RSSfeed\\_IWK\\_All](http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=228400096&cid=RSSfeed_IWK_All)

### **CRITICAL MANUFACTURING**

**Glitch pops up in Toyota Camry recall.** Toyota said it will fix accelerator pedal assemblies in the Avalon, Camry, and Camry Hybrid that may have been damaged in the company's big recall for unintended acceleration. But it said the matter is a secondary repair and not another recall. The technical service bulletin instructs Toyota dealership technicians how to repair two weld nuts that "may be damaged" in the recall repair. "Suggestions that this TSB was issued to resolve customer complaints about accelerator pedal feel after the recall or that this TSB is a recall are wrong," Toyota said in a statement. "No TSB is planned for other models since this component is unique to the Camry and Avalon platform." However, Consumer Reports said on its Web site that "as many as 500 owners of those cars have complained of gas pedals that feel loose or have play side-to-side." The new TSB applies to 2005-'10 Avalons and 2007-'10 Camry and Camry Hybrid cars that were subject to the original recall. That recall dealt with accelerator pedals that could become stuck in place or trapped by floor mats. Toyota said technicians may have accidentally stripped bolts on the accelerator bracket of those vehicles during repairs related to the recall. Source:

<http://www.insideline.com/toyota/camry/glitch-pops-up-in-toyota-camry-recall.html>

**National Highway Traffic Safety Administration investigating repairs of recalled rental cars.** Federal regulators are investigating how quickly rental car companies repair vehicles subject to a safety recall. The National Highway Traffic Safety Administration sent letters in mid-November to GM, Chrysler, and Ford asking for records on recall repairs for 2.9 million cars owned by rental companies. The agency's office of defects investigation said the audit was prompted by "recent allegations of crashes and deaths from un-remedied recalled vehicles." In June, a jury hearing a wrongful death lawsuit against Enterprise Rent-A-Car of San Francisco, California awarded \$15 million in damages to the parents of two sisters from Santa Cruz, California. The sisters died in 2004 when their rented PT Cruiser caught fire and hit a truck. The car was subject to a safety recall for a power steering hose defect that could cause a fire under the hood; it had not been repaired. Enterprise, the nation's largest rental car company, and its corporate parent admitted they were negligent and that "their negligence was the sole proximate cause of the fatal injuries," according to a document signed by their attorneys in the case. Source: [http://www.mercurynews.com/breaking-news/ci\\_16736705](http://www.mercurynews.com/breaking-news/ci_16736705)

UNCLASSIFIED

## UNCLASSIFIED

**U.S. Dept. of Transportation wants to disable phones in cars.** The Secretary of Transportation said the U.S. Department of Transportation (DOT) wants to make it impossible to use cellular phones while in moving vehicles through the use of blocking technology. "I think the technology is there," he said. "And I think you're going to see the technology become adaptable in automobiles to disable these cell phones." The move is being considered due to the rising number of traffic deaths (about 5,500) and injuries (500,000) that result each year from distracted driving. Right now, there are no federal laws to prevent drivers from using cell phones, though a number of states and municipalities have enacted such legislation. The Secretary, however, does not think the laws are a big enough deterrent. He indicated that jamming equipment would not be used, but instead the DOT is considering software solutions from companies such as Zoomsafter, tXtBlocker, and iZup, which disable certain phone features when it is determined that they are in a moving vehicle. The Secretary did not provide any sort of time frame. Source:

<http://www.phonescoop.com/news/item.php?n=7037>

**Boeing to rework 787 electric system after fire.** Boeing Co. will have to rework part of the software on the 787 Dreamliner's electrical system and its power panels after an onboard fire 2 weeks ago halted flight tests, three people familiar with the matter said. A stray aluminum washer inside a power panel shorted out during a November 9 flight, causing the blaze. The 787 test fleet will stay grounded in the meantime. The company plans to modify the Dreamliner's power panels to make sure stray materials cannot get inside, and will also change the electrical system's software to improve power distribution. Source:

<http://news.cincinnati.com/article/20101128/BIZ/11280301/1076/Boeing-to-rework-787-electric-system-after-fire>

## **DEFENSE/ INDUSTRY BASE SECTOR**

**(Maine) Navy expected to reduce funds for shipyard maintenance work.** Despite a report from a federal watchdog agency indicating the U.S. Navy drastically under funds maintenance work at its Portsmouth Naval Shipyard in Kittery, Maine, the Navy is expected to provide even less funding than it currently does at least through 2016. That was the message delivered the week of November 22 to shipyard and union officials by the commander of Naval Sea Systems Command. "He made it clear to us there's less money next year than this year, and with a tightening for the next few years," said the president of the Metal Trades Council at the yard. "The problem is we're already woefully underfunded for any maintenance. The work will have to come out of our existing budget and our existing budget is allocated for mission essentials." The cuts are to the restoration and modernization, or facilities maintenance, budget. There will not be any cuts to the shipyard workforce. Source: <http://www.seacoastonline.com/articles/20101128-NEWS-11280323>

## **EMERGENCY SERVICES**

**(Washington) Seattle police to tweet stolen car descriptions.** The Seattle, Washington police department said December 1 it will start tweeting information on stolen vehicles in an effort to curb rising auto theft rates. It will publish the color, year, make, model, body style, and license plate numbers on a Twitter account dubbed "Get your car back." Seattle police said the average number of cars stolen per day in the city has risen from 8.46 last year to 9.9 this year, and more than 3,000 were

UNCLASSIFIED

## UNCLASSIFIED

stolen through October. Employees at the 911 Seattle call center will tweet a car's information after it is reported stolen. The department is encouraging Twitter followers who spot stolen cars to call police but not to contact any occupants. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/02/AR2010120202183.html>

**(Washington) Package prompts evacuation of Bainbridge Island police station.** A suspicious package brought to the Bainbridge Island Police Department in Washington November 29 prompted an emergency evacuation. A woman who found an unrecognized container in her car brought it to the station, said a police lieutenant. Fearing the package contained explosives, police contacted the Washington State Patrol (WSP). WSP X-rayed the item on the scene and determined it did not contain any explosives. The police station, as well as all neighboring structures within 500 feet, were evacuated during the incident. The origin of the package has not been determined. Source: <http://www.komonews.com/news/local/111008424.html>

## **ENERGY**

**U.S. drops bid to explore oil in Eastern Gulf.** The Presidential administration announced December 1 it had rescinded its decision to expand offshore oil exploration into the eastern Gulf of Mexico and along the Atlantic Coast because of weaknesses in federal regulation revealed by the BP oil spill. The Interior Secretary said that a moratorium on drilling would be in force in those areas for at least 7 years, until stronger safety and environmental standards were in place. The move puts off limits millions of acres of the Outer Continental Shelf that hold potentially billions of barrels of oil and trillions of cubic feet of natural gas. The decision essentially reverses the much-disputed drilling plan announced in March, which would have initiated environmental studies and exploration activity in previously untouched areas off the Gulf Coast of Florida and along the East Coast from Florida to Delaware. Source: <http://www.nytimes.com/2010/12/02/us/02drill.html? r=1&partner=rss&emc=rss>

**(Massachusetts) Power outage affected 30,000 on North Shore.** A combination of equipment failure and bad weather left about 30,000 National Grid customers on the North Shore of Massachusetts without power December 1, according to a National Grid official. Parts of several different communities north of Boston lost power between 5 and 5:30 p.m., a National Grid spokeswoman said. Other than weather and equipment failure, she could not name a specific cause for the outage. Cities and towns affected included East Beverly, Gloucester, Rockport, Essex, Manchester, Hamilton, and Wenham. Power was restored between 8:30 and 9 p.m. Source: [http://www.boston.com/yourtown/news/beverly/2010/12/30000\\_in\\_the\\_north\\_shore\\_lost.html](http://www.boston.com/yourtown/news/beverly/2010/12/30000_in_the_north_shore_lost.html)

**(New York) New York power outage.** More than 31,000 utility customers across New York had their power knocked out by high winds from the storm December 1. For some, power was still out December 2. According to NYSEG's Web site there are still multiple power outages across the state and in parts of the Southern Tier. In areas where snow had accumulated, the winds created treacherous driving conditions for motorists. Source: <http://www.wetmtv.com/news/local/story/New-York-Power-Outage/haEIZGhJ2kauaUptPBI6eQ.csp>

**(Pennsylvania) Pa. copper thieves caused gas explosion at home.** A state police fire marshal believes thieves intentionally caused a natural gas explosion after stealing a copper natural gas line and other copper utility lines from a vacant home in southwestern Pennsylvania. Copper thefts are common

UNCLASSIFIED

## UNCLASSIFIED

because the metal is easily sold for scrap. A fire marshal out of the Belle Vernon barracks said someone cut copper lines out of the home in Redstone Township November 27. That caused a gas leak and it appears the thieves then ignited the gas in a way authorities are not revealing. Troopers arrived to find the gas still leaking and evidence of an explosion which blew out windows, doors, and other household items into yards nearby. Police have not named or arrested any suspects. Source: [http://www.ldnews.com/news/ci\\_1674168](http://www.ldnews.com/news/ci_1674168)

**(Nebraska) Copper theft was inside job, OPPD says.** Omaha, Nebraska investigators said the theft of \$14,000 in copper from an Omaha Public Power District (OPPD) substation was an inside job. A former employee has been charged with felony theft. Investigators said the suspect cashed in on the thefts during the past year and a half, and they believe he worked alone. Police believe the suspect stole 3,200 pounds of copper and aluminum during the past 18 months. "He knew what he was doing what money he could get from this," said a Douglas County Sheriff's Office spokesman. Source: <http://www.ketv.com/r/25951952/detail.html>

**(Nebraska) Power outage result of multiple problems.** Multiple issues within Sidney, Nebraska's electric grid was the cause behind a pre-Thanksgiving power fiasco that lasted more than 7 hours. According to a report by the Electric Department superintendent, the power outage began at 10:50 p.m. November 24, when a main line from the south substation near the Lodgepole Valley Youth Camp burned down. Crews switched feeders out of the power plant and the substation to restore power, but a breaker in the North Side substation tripped, taking out power to central Sidney. While crews repaired the damage at the south substation, system frequencies somehow changed and began to trip the 115 KV circuit switcher, which feeds the North Side substation. City crews ended up repairing all three conductors at the Lodgepole Valley Youth Camp. Power was restored at 6:15 a.m. November 25, with the final outage at the city's blending tank, which had power restored at 6:40 a.m. Source: <http://www.suntelegraph.com/cms/news/story-202363.html>

**Flows on Enbridge oil line seen cut until November 30.** Enbridge Inc's 670,000 barrel per day Line 6A oil pipeline in the U.S. Midwest was expected to run at reduced rates until November 20, creating another costly bottleneck for Canadian crude exports, the company said November 26. An outage at a power utility's substation in Illinois forced Enbridge, which has been struggling with numerous outages on its massive oil pipeline system, to reduce flows as electricity to a pumping station got cut off. Market sources said flows on the pipeline to Griffith, Indiana, from Superior, Wisconsin, have been chopped by about one third from already-reduced volumes. The power outage occurred November 25 at Lockport, Illinois, near Chicago. The incident happened on the same day Enbridge restarted the 290,000 barrel per day Line 6B, which was shut for about 1 week as the company investigated possible problem spots it found during an in-line inspection. Source: <http://www.reuters.com/article/idUSN2612255320101126>

## **FOOD AND AGRICULTURE**

**(New York) Health alert now a recall for NY Gourmet Salads.** NY Gourmet Salads, Inc., a deli supplier and caterer in Brooklyn, New York is recalling various meat and poultry products produced without federal inspection, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced December 2. The company's ready-to-eat deli products were also the subject of a public health alert issued October 30. After a continued investigation by FSIS, the firm recalled its products.

UNCLASSIFIED

## UNCLASSIFIED

NY Gourmet Salads and the government have been at odds for months, and the U.S. Department of Justice announced in August it was seeking a permanent injunction against the company and its president. In the complaint, the defendants were charged with selling food that was prepared, packed, or held under unsanitary conditions, and that may have become contaminated with filth or may have been injurious to health. Inspections over many years, including one in March found *Listeria monocytogenes* throughout the manufacturing facility. Source:

<http://www.foodsafetynews.com/2010/12/more-problems-for-brooklyn-salad-maker/>

**Monsanto GMO sugarbeets to be destroyed: court.** A federal judge November 30 ordered the destruction of plantings of genetically modified sugar beets developed by Monsanto Co after ruling previously the U.S. Agriculture Department (USDA) illegally approved the biotech crop. A U.S. District Court judge in August banned the planting and sales of Monsanto's "Roundup Ready" biotech sugar beets after determining that their approval in 2005 by the USDA was illegal. He said the government must conduct a thorough environmental review before approving the crop to comply with the law. But shortly after the ruling, the USDA issued permits allowing companies to plant seedlings to produce seed for future Genetically modified organism (GMO) sugar beet crops. In his ruling, the judge said those seedlings "shall be removed from the ground." Earthjustice, a consumer group that brought the case against the USDA and had asked the judge to order the young plants be destroyed, said the action was the first court-ordered destruction of a GMO crop. Sugar beets account for more than half of the nation's sugar supply, and Monsanto's Roundup Ready beets have been popular with farmers as they have been genetically altered to withstand sprayings of the chemical herbicide Roundup, making weed management easier for producers. Source:

<http://www.reuters.com/article/idUSTRE6B00Y520101201>

**Salmonella prompts nutmeg recall.** Frontier Natural Products Co-op is recalling nutmeg it received from a New Jersey supplier because it may be contaminated with Salmonella. Mincing Overseas Spice Company of Dayton, New Jersey, supplied the nutmeg being sold under Frontier Natural Products Co-op and Whole Foods Markets brands. The recalled products, Frontier Bulk 16 oz. ground nutmeg with the UPC Code: 0-89836-00165-8, Lot Code 0306 and Whole Foods 365 brand 1.92 oz. ground nutmeg with the UPC Code: 0-99482-41931-8, Lot Code 0321, were sold in all 50 states and some parts of Canada to distributors, retailers, and consumers. Source:

<http://www.foodsafetynews.com/2010/12/salmonella-fear-leads-to-nutmeg-recall/>

**Senate approves long-delayed food safety bill.** The U.S. Senate passed a food safety bill November 30 to give more power to the Food and Drug Administration (FDA), more than a year after the House of Representatives passed a similar measure. The bill, designed to bolster the safety of the nation's food supply, passed 73 to 25. A version of the bill was passed by the House of Representatives in July of 2009 but had languished in the Senate, a fact that has angered some food safety advocates. At that time, the Center for Science in the Public Interest said there had been 85 recalls of FDA-regulated foods since the House of Representatives passed their version of the bill. The recalls were associated with 1,850 reported illnesses, the report said. The bill, called the Food Safety Enhancement Act (S. 510), covers many aspects of food safety, including better preventive control measures by manufacturers, more frequent inspections of facilities, and greater FDA authority over recalls. The bill is supposed to help the government and food manufacturers handle situations like recent recalls on lettuce, peanuts, and eggs. The bill will allow the FDA to order direct recalls instead of relying on

UNCLASSIFIED

## UNCLASSIFIED

voluntary recalls by manufacturers. Source:

<http://www.cnn.com/2010/POLITICS/11/30/food.safety.bill/index.html?hpt=C1>

**(Georgia) Counties declared ag disasters.** More than 150 Georgia counties have been declared agricultural disaster areas as excessive heat and drought took a toll on crops over the summer. To qualify, counties had to have sustained production losses of 30 percent or greater because of the drought. The disaster designation by the U.S. Department of Agriculture (USDA) allows farmers in the designated counties to be considered for low-interest emergency loans from the department's Farm Service Agency. In a news release, Georgia's governor praised the USDA decision to "do everything in our power to assist farmers in counties that have been hit hard by dry weather and extreme heat in the past several months." Soybean, corn, and cattle farmers all took a hit over the summer. Farmers in qualified counties have until July 26, 2011, to apply for emergency loan assistance. Source:

<http://www.timesfreepress.com/news/2010/nov/30/counties-declared-ag-disasters/>

**Asian carp create nagging fear in Lake Erie towns.** The Great Lakes are already ravaged by exotic species such as the sea lamprey and quagga mussel. The Asian carp could be next. Scientists are unsure how much damage they could do, but some fear the carp would crowd out competitors and decimate a \$7 billion fishing industry. The carp are greedy giants that suck plankton from the water with the efficiency of vacuum cleaners. The danger is greatest in Lake Erie, which has the most abundant fish populations of the five lakes and a plentiful supply of plankton, the foundation of the food chain. Commercial fishing is still alive in Canadian port towns scattered along the lake's northern shoreline. Local fishermen are already squeezed by the economy and catch regulations, and they fear Asian carp could devastate their livelihood. Source:

<http://www.businessweek.com/ap/financialnews/D9JNMIO81.htm>

**(Alaska) Fish processor will recall salmon.** The owner of a Fairbanks, Alaska, fish processing company said three samples of the same batch of smoked salmon the state deemed contaminated were tested by independent laboratories in the lower 48 states and came back negative. But the owner said he will comply with the state's order for a recall of Santa's Smokehouse brand Cajun-Style Smoked Keta Salmon. "We're required by law to issue a recall," he said. The fish is produced by Interior Alaska Fish Processors Inc. The fish was sold in half-pound packages between August 27 and November 6. The Alaska Department of Environmental Conservation found the bacterium *Listeria monocytogenes* in a batch sold at the company's retail stores. Source: <http://www.necn.com/11/28/10/Fish-processor-will-recall-salmon/landing.html?&blockID=3&apID=0e9fc1fa23bc4b4780e65a31907d879c>

## **GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

**(Connecticut) Propane delivery driver arrested after fire at Coventry High School.** A propane delivery driver has been arrested after police said his actions resulted in a flash fire at Coventry High School in Coventry, Connecticut. The 42-year-old driver, of Preston, was the only person injured in the fire. He sustained minor burns. Police said the man was delivering two 120-gallon propane cylinders to the school outside of a fully-occupied cafeteria at lunchtime November 29 when the incident occurred. Before filling the cylinders, the man intentionally opened the supply line/nozzle from his truck, venting propane to the area at the side of the cafeteria, according to police. Police said the vented propane traveled through the school wall, igniting from a source in the kitchen on the other side and

UNCLASSIFIED

## UNCLASSIFIED

causing a large, exterior flash fire. The suspect has been charged with second-degree reckless endangerment and a violation of the Connecticut Liquefied Petroleum Gas Code. He was released on a promise to appear in court in Rockville December 14. Source:

<http://www.ctnow.com/news/connecticut/tolland/hc-coventry-fire-arrest-1202-20101201,0,7222583.story>

**(Georgia) Clayton State lock down lifted after bomb threat.** A lockdown at Clayton State University in Morrow, Georgia, has been lifted following a bomb threat. A university spokesman said authorities found no suspicious packages on campus December 1 after a building-by-building sweep. The search was completed just before 5 p.m. The spokesman said the bomb threat call came into Morrow's 911 center about 1 p.m. but was not about any specific location on campus. He said evening classes would go on as scheduled. Clayton State is just south of Atlanta in Morrow. Source:

<http://www.cbsatlanta.com/news/25995088/detail.html>

**(Iowa) Hack of alert system shows vulnerabilities.** Computer hackers have broken into an Iowa state government Web site for the third time this year, exposing continued vulnerabilities in the state's digital security programs. The latest incident occurred November 27 when a hacker breached a server used by the Iowa Department of Public Safety to issue Amber Alert bulletins involving child abduction cases. The hacker used the access at 8:18 a.m. to reissue an Amber Alert warning from February about a Council Bluffs teenager who was missing and later found safe. The bulletin was canceled at 8:23 a.m. and there is no indication that any search was launched to find the girl. The Iowa Division of Criminal Investigation's cybercrime unit is investigating in cooperation with the Iowa Department of Administrative Services, a spokeswoman said. Source:

<http://www.desmoinesregister.com/article/20101201/NEWS/12010342/-1/watchdog/Hack-of-alert-system-shows-vulnerabilities>

**U.S. cuts access to files after leak embarrassment.** The U.S. State Department severed its computer files from the government's classified network, officials said November 30, as U.S. and world leaders tried to clean up from the embarrassing leak that spilled America's sensitive documents onto screens around the globe. By temporarily pulling the plug, the U.S. significantly reduced the number of government employees who can read important diplomatic messages. It was prompted by the disclosure of hundreds of thousands of those messages this week by WikiLeaks, the self-styled whistleblower organization. The documents revealed that the U.S. is still confounded about North Korea's nuclear military ambitions, that Iran is believed to have received advanced missiles capable of targeting Western Europe and — perhaps most damaging to the U.S. — that the State Department asked its diplomats to collect DNA samples and other personal information about foreign leaders.

Source: [http://news.yahoo.com/s/ap/20101130/ap\\_on\\_go\\_ca\\_st\\_pe/wikileaks](http://news.yahoo.com/s/ap/20101130/ap_on_go_ca_st_pe/wikileaks)

**GAO finds gaps in wireless security at federal agencies.** The U.S. Government Accountability Office (GAO) found several gaps in the security of wireless networks used by federal agencies and made several recommendations to enhance safety, according to a report published November 30. U.S. federal networks, including the Pentagon, have increasingly become targets of cyber attacks and hacking. The Pentagon is currently stepping up its cyber security system after hackers hijacked the Internet for over 15 minutes earlier in November. Given such intrusions in cyber security, the GAO was asked to suggest several updates to its previous report on information security. "Existing government-wide guidelines and oversight efforts do not fully address agency implementation of

UNCLASSIFIED

## UNCLASSIFIED

leading wireless security practices,” the GAO said. The GAO conducted detailed testing at the Departments of Agriculture, Commerce, Transportation, Veterans Affairs, and the Social Security Administration. Source: <http://www.ibtimes.com/articles/87462/20101201/gao-internet-wireless-security-pentagon.htm>

**WikiLeaks fallout: White House orders security clampdown.** The U.S. President’s administration November 29 ordered all federal agencies that deal with sensitive information to review and enhance their internal security programs in an effort to staunch the flow of unauthorized documents to WikiLeaks and other rogue Web sites. Among other things, the administration is ordering agency heads to develop stricter criteria for determining which federal employees are given access to secured computer systems and networks that store classified data. “Our national defense requires that sensitive information be maintained in confidence to protect our citizens, our democratic institutions, and our homeland,” said the Office of Management and Budget director, in a letter to agency heads. Several newspapers, including The New York Times, Der Spiegel, The Guardian, and Le Monde, over the weekend published stories that disclosed the contents of classified, U.S. government documents first obtained by WikiLeaks. Source:

[http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=228400135&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/news/security/management/showArticle.jhtml?articleID=228400135&cid=RSSfeed_IWK_News)

**(Michigan) Police: Attack against Wayne State University thwarted.** A violent attack planned on the campus of Wayne State University (WSU) in Detroit, Michigan has been thwarted by police. Officers and the FBI raided the home of the student from Dearborn, Michigan, who made the threats. The student has been banned from the WSU campus but has not been identified. A statement from the university said no weapons or ammunition were found in the search of the student’s residence.

Source: <http://wtvbam.com/news/articles/2010/nov/30/police-attack-against-wayne-state-university-thwar/>

**(Wisconsin) Police: School suspect fired at least 5 times, had more bullets.** A 15-year-old sophomore, accused of holding 23 classmates and a teacher hostage for about 5 hours November 29 at his Marinette, Wisconsin high school, fired his two weapons at least five times and had a duffel bag containing more bullets with him, authorities said November 30. The alleged hostage-taker died November 30 at a hospital of a self-inflicted gunshot wound, authorities said. The teen turned one of his guns on himself as police broke into the Marinette High School classroom after hearing gunshots. All 24 hostages were unharmed. The Marinette police chief said police are still trying to determine a motive, saying the student was well-liked, had no prior law enforcement contact, and “was a good student.” Five or six shell casings from both weapons — a .22-caliber semi-automatic and a 9-millimeter semi-automatic — were found in the classroom. Bullets were also found in the suspect’s pocket at the hospital, and a duffel bag left in the classroom contained “numerous live rounds,” the chief said. A bomb squad was called in to X-ray and remove the bag. The school was closed November 30. Source: <http://www.cnn.com/2010/CRIME/11/30/wisconsin.hostage/index.html?hpt=T2>

**(California) FBI probe claims of AIDS-tainted razors sent to UCLA professor.** The FBI and local police November 24 were investigating another incident involving a University of California, Los Angeles (UCLA) neuroscientist, this one involving an animal-rights group that claims to have sent “AIDS-tainted” razors to the researcher. Officials said they do not know whether the razors had any substance on them, but that they are trying to find out. Earlier in November, a researcher, who does

UNCLASSIFIED

## UNCLASSIFIED

research on rodents and primates, received the package, a UCLA spokesman said. Previously, animal-rights activists have demonstrated in front of the researcher's house and allegedly set fire to his car. In a news release issued November 23, the Animal Liberation Front said it had obtained statements from animal activists called "The Justice Department of UCLA," which claimed responsibility for sending AIDS-tainted razor blades to the researcher, whom the group alleged has injected the rodents with addictive drugs. Much of the research is funded by the National Institutes of Health and has provided key information on biochemical processes that contribute to methamphetamine addiction affecting teens, and disabilities affecting speech and behavior of schizophrenia patients, UCLA said. Source: <http://latimesblogs.latimes.com/lanow/2010/11/fbi-probes-allegedly-aids-tainted-razors-sent-to-ucla-professor.html>

**(Hawaii) 2 men arrested; SUV searched for bombs near military housing.** Police in Honolulu, Hawaii, shut down the Ala Kapuna off-ramp along Moanalua Freeway Honolulu-bound for about 2 hours November 27 to investigate a suspicious vehicle that may contain explosives, police dispatch reported. An Army spokesman said two men had been arrested in connection with the case. The chief of public affairs for U.S. Army Pacific would not elaborate, but he said the men had apparently tried to get into the Aliamanu Military Reservation housing area. They earlier tried to get onto other military installations on Oahu, he said. A black mid-size sport utility vehicle was stopped at the gate while the investigation continued. The two men were spotted trying to enter at least two other "Leeward Oahu military bases" that he would not name. Police also closed Ala Kapuna Street, starting at the overpass, heading to mauka and the mauka gate to Aliamanu military housing. The off-ramp, overpass, and gate were reopened just after 5:25 p.m. It was not clear if any explosives were found in the SUV. Source: [http://www.staradvertiser.com/news/breaking/Suspicious\\_vehicle\\_near\\_freeway\\_may\\_contain\\_explosives.html](http://www.staradvertiser.com/news/breaking/Suspicious_vehicle_near_freeway_may_contain_explosives.html)

**Clinton: U.S. 'deeply regrets' WikiLeaks disclosures.** The U.S. Secretary of State condemned the release of more than 250,000 classified State Department documents November 29, saying the United States was taking aggressive steps to hold responsible those who "stole" the information. In her first public comments since the November 28 release of the classified State Department cables, she said online whistleblower Wikileaks acted illegally in posting the material. She said the U.S. Presidential administration was "aggressively pursuing" those responsible for the leak. Her comments come as the Presidential administration moved into damage control mode, trying to contain fallout from unflattering assessments of world leaders and revelations about backstage U.S. diplomacy. The publication of the secret cables amplified widespread global alarm about Iran's nuclear ambitions and unveiled occasional U.S. pressure tactics aimed at hot spots in Afghanistan, Pakistan, and North Korea. According to the vast cache of cables, a Saudi Arabian leader repeatedly urged the United States to attack Iran's nuclear program, and China directed cyber attacks on the United States. The documents, given to five media groups by the whistle-blowing Web site WikiLeaks, provide candid and at times critical views of foreign leaders as well as sensitive information on terrorism and nuclear proliferation filed by U.S. diplomats, according to The New York Times. The White House condemned the release, and said the disclosures may endanger U.S. informants abroad. Source: [http://www.msnbc.msn.com/id/40412689/ns/us\\_news-security](http://www.msnbc.msn.com/id/40412689/ns/us_news-security)

UNCLASSIFIED

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**AVG update crashes 64-bit Windows 7 systems.** The latest software update from security supplier AVG Technologies has caused problems with many users running Microsoft's 64 bit Windows 7 operating system. The conflict between update 3292 for both free and paid-for versions of the software causes systems to go into an infinite crash loop, the company said. AVG has withdrawn the update and published an advisory on how to get affected systems running again and links to FAQs. AVG also said it will release a program to ensure the fix is completed automatically as soon as possible. Users who are running Windows 7 and have not downloaded and installed update 3292 will be unaffected, the company said. Source:

<http://www.computerweekly.com/Articles/2010/12/03/244315/AVG-update-crashes-64-bit-Windows-7-systems.htm>

**Google quashes 13 Chrome bugs, adds PDF viewer.** Google December 2 patched 13 vulnerabilities in Chrome as it shifted the most stable edition of the browser to version 8. Chrome 8 also debuted Google's built-in PDF viewer, an alternative to the bug-plagued Adobe Reader plug-in, and included support for the still-not-launched Chrome Web Store. The 13 flaws fixed in Chrome 8.0.552.215 are in a variety of components, including the browser's history, its video indexing, and the display of SVG (scalable vector graphics) animations. Four of the baker's dozen are tagged as "high" level bugs, Google's second-most-serious rating, while five are pegged "medium" and four are labeled as "low." Source:

[http://www.computerworld.com/s/article/9199418/Google\\_quashes\\_13\\_Chrome\\_bugs\\_adds\\_PDF\\_viewer](http://www.computerworld.com/s/article/9199418/Google_quashes_13_Chrome_bugs_adds_PDF_viewer)

**Malicious Kodak galleries used for serving Trojan.** A variant of a highly specialized Trojan has appeared on fake sites mimicking Kodak Gallery pages, where potential victims are urged to download software that would supposedly allow them to watch the offered slideshow, but actually creates a folder with configuration files and copies a few executables into the System32 folder. But before doing that, it actually does show the users a slideshow of car pictures, which acts as a smokescreen in order to hide the malicious activity. Further research by Sunbelt's experts revealed the fact the pictures are of a car might not be so random. The Bayrob Trojan — of which this is a variant — has had a history of targeting eBay users, especially those buying motors and cars since that means that bigger amounts of money are involved. The Trojan spoofs various eBay pages and tries to trick the users into parting with their money. Source: [http://www.net-security.org/malware\\_news.php?id=1552](http://www.net-security.org/malware_news.php?id=1552)

**Facebook hit with likejacking, Zeus malware attack.** Facebook users have once again been hit with a Likejacking ploy and Zeus variant. In the latest scam, detected by researchers at Sophos, users receive a message, allegedly coming from a friend, coupled with a link to a YouTube knock-off site called "FouTube." However, the Facebook "Like" option leads to a likejacking scam. Instead of spreading malware, the attack displays a survey and tricks users to subscribe to an exorbitant SMS services rate on their mobile phones. Meanwhile, a Trend Micro anti-spam research engineer warned another malware attack is circulating on the site, entailing spammed messages appearing to come from Facebook and falsely warning users their IP addresses were sending numerous spam messages to different e-mail addresses. The message then suggests that users download an offered freeware tool,

## UNCLASSIFIED

called FB IPsecure, which claims to be from Facebook so they can put a stop to the spammed messages coming from their machine. The download is actually a malicious Zeus variant, aimed at taking control of a user's computer once installed. Source:

<http://www.crn.com/news/security/228500108/facebook-hit-with-likejacking-zeus-malware-attack.htm?itc=refresh>

**Canon image originality verification proven useless.** ElcomSoft discovered a vulnerability in Canon's Original Data Security System, a validation system to guarantee authenticity of digital images captured with supported Canon cameras. The vulnerability opens the possibility to produce images that will be positively validated by Canon's own Original Data Security Kit (OSK-E3) regardless of whether or not the images are, in fact, genuine. After performing analysis of Canon hardware, ElcomSoft researchers were able to extract secret keys used to calculate authentication data from Canon EOS digital cameras, and use the keys for adding authenticity signatures to a set of manipulated digital images. The vulnerability exists in all Canon cameras manufactured to this day that have the security feature. ElcomSoft made Canon aware about the vulnerability by notifying the vendor as well as the CERT Coordination Center as a trusted third-party. Source: <http://www.net-security.org/secworld.php?id=10221>

**Feds pursue Russian, 23, behind 1/3 of all world spam.** FBI investigators have named a 23-year-old Russian as a prime suspect behind the operation of the infamous 500,000 Mega-D botnet, blamed for an estimated one in three spam e-mails prior to a take-down operation early last year. The 23-year-old Moscow resident was accused of violating U.S. anti-spam and fraud laws in a sworn testimony by an FBI agent investigating the case, the Smoking Gun reports. Webmail records from two Gmail accounts and financial transactions (via the ePassporte service) link the suspect to the operation of the botnet, according to court paper submitted in a grand jury investigation. He is the first suspect to be named in the Mega-D botnet investigation. Source:

[http://www.theregister.co.uk/2010/12/01/mega\\_d\\_botnet\\_suspect\\_named/](http://www.theregister.co.uk/2010/12/01/mega_d_botnet_suspect_named/)

**Ransomware attack resurfaces to hold files hostage.** The latest ransomware attack seems to be a variant of the GpCode Trojan that has made seemingly annual reappearances to extort money for the past few years. A compromised system will show a Notepad pop-up, or change the desktop background to display a message that reads "Attention!!! All your personal files were encrypted with a strong algorithm RSA-1024 and you can't get an access to them without making of what we need!" This message is followed by more broken English instructions directing the user to read a text file explaining that a ransom of \$120 is required to get the decryption key. Past ransomware extortion efforts created an encrypted copy of the file, but left the original intact. This latest version, however, encrypts the original file — making any recovery efforts significantly harder, if not virtually impossible. Users are directed to shut the computer down as quickly as possible once the ransom alert appears. In the background, the malware is still busy doing its dirty work, and by shutting the system down — yanking the plug from the wall if necessary — the user might be able to save some of the data. Source: <http://www.networkworld.com/news/2010/112910-ransomware-attack-resurfaces-to-hold.html?hpg1=bn>

**Scammers can hide fake URLs on the iPhone, says researcher.** Identity thieves can hide URLs on the iPhone's limited screen real estate, tricking users into thinking they are at a legitimate site, a security researcher said November 29. In a proof-of-concept, the researcher showed how legitimate Web

UNCLASSIFIED

## UNCLASSIFIED

applications such as Bank of America's mobile banking application hide Safari's address bar after rendering the page. He speculated that developers use this practice to use as much as possible of the limited screen real estate on mobile devices like the iPhone. "Note that on the iPhone, this only happens for sites that follow directives in HTML to advertise themselves as mobile sites," said the researcher on his personal blog and in an entry on the SANS Institute's blog. The ability to hide the address bar in iOS is by design, noted the researcher. "I did contact Apple about this issue and they let me know they are aware of the implications, but do not know when and how they will address the issue," the researcher said. He suggested that Apple modify iOS to prevent Web applications from hiding the URL. Source:

[http://www.computerworld.com/s/article/9198380/Scammers can hide fake URLs on the iPhone says researcher](http://www.computerworld.com/s/article/9198380/Scammers_can_hide_fake_URLs_on_the_iPhone_says_researcher)

**Security researcher warns on fake trojan removal kit.** A security researcher has issued a warning about a fake trojan removal kit that infects Windows users with the ThinkPoint Rogue malware. Writing in his security blog November 29, the researcher said the "Windows Trojan Removal Kit" effectively hijacks users' PCs using the ThinkPoint Rogue malware. This malware, the Sunbelt Software/GFI Software researcher said, only has a close to 50 percent detection rate in the IT security software stakes. The file, he said, is currently being offered up by typical "fake security scan" pages, such as microsoftwindowssecurity152(dot)com. Installing the executable can potentially cause fake "Blue Screens of Death" and payment nag screens to appear. He has posted details on his blog about how to work around the supposed locked up desktop, and how the malware appears to be flagging itself as Trojan.Win32.Generic.pak!cobra, a malware infection that was originally discovered at the start of this year. Source: <http://www.infosecurity-magazine.com/view/14302/security-researcher-warns-on-fake-trojan-removal-kit/>

**'Nightmare' kernel bug lets attackers evade Windows UAC security.** Microsoft is investigating reports of an unpatched vulnerability in the Windows kernel that could be used by attackers to sidestep an important operating system security measure. One security firm dubbed the bug a potential "nightmare," but Microsoft downplayed the threat by reminding users that hackers would need a second exploit to launch remote attacks. The exploit was disclosed November 24 — the same day proof-of-concept code went public — and lets attackers bypass the User Account Control (UAC) feature in Windows Vista and Windows 7. UAC, which was frequently panned when Vista debuted in 2007, displays prompts that users must read and react to. It was designed to make silent malware installation impossible, or at least more difficult. The bug is in the "win32k.sys" file, a part of the kernel, and exists in all versions of Windows, including XP, Vista, Server 2003, Windows 7, and Server 2008, a Sophos researcher said in a November 25 blog post. Several security companies, including Sophos and Vupen, have confirmed the vulnerability and reported that the publicly-released attack code works on systems running Vista, Windows 7, and Server 2008. Source:

[http://www.computerworld.com/s/article/9198158/Nightmare kernel bug lets attackers evade Windows UAC security](http://www.computerworld.com/s/article/9198158/Nightmare_kernel_bug_lets_attackers_evade_Windows_UAC_security)

**Leaked U.S. document links China to Google attack.** The cache of more than 250,000 U.S. Department of State cables that WikiLeaks began releasing November 28 includes a document linking China's Politburo to the December 2009 hack of Google's computer systems. The U.S. Embassy in Beijing was told by an unidentified Chinese contact that China's Politburo "directed the intrusion into Google's computer systems," the New York Times reported November 28, citing a single leaked State

UNCLASSIFIED

## UNCLASSIFIED

Department cable. “The Google hacking was part of a coordinated campaign of computer sabotage carried out by government operatives, private security experts, and Internet outlaws recruited by the Chinese government. They have broken into American government computers and those of Western allies, the Dalai Lama and American businesses since 2002, cables said,” the Times reported. The cable is another piece of evidence, albeit thinly sourced, linking China to the Google attack. Security experts have linked the attacks to servers at a university used by the Chinese military, and both Google and the State Department implied that they thought China was behind the attacks when they were first disclosed in January 2010, but nobody has produced conclusive proof that they were state-sponsored. Source:

[http://www.computerworld.com/s/article/9198198/Leaked\\_U.S.\\_document\\_links\\_China\\_to\\_Google\\_attack](http://www.computerworld.com/s/article/9198198/Leaked_U.S._document_links_China_to_Google_attack)

**Feds seize 70 ‘filesharing, dodgy goods’ sites.** The U.S. government has seized 70 sites allegedly offering counterfeit goods or links to copyright-infringing material. Among the domains seized was a BitTorrent meta-search engine Torrent-Finder.com, along with other music linking sites. Other sites on the hitlist allegedly sold fake designer clothes. Surfers visiting the seized sites were confronted by a notice from Immigration and Customs Enforcement (ICE), instead of the expected content. ICE told the New York Times the seizures were part of an “ongoing investigation” but declined to elaborate, beyond saying court-issued seizure warrants were involved. The seizures happened as a new bill addressing this issue, the Combating Online Infringements and Counterfeits Act, has been introduced in Congress. Source: [http://www.theregister.co.uk/2010/11/29/ice\\_piracy\\_domain\\_seizures/](http://www.theregister.co.uk/2010/11/29/ice_piracy_domain_seizures/)

**Fake Facebook ‘photo comment’ e-mail leads to malware.** As Facebook has announced its new messaging system and its deployment in the coming months, online scammers have been trying to use that announcement against unsuspecting Facebook users that may have heard about it and believe that changes will be made in the way that the social network contacts and notifies its users. McAfee warns about the latest of these scams — a fake “Your friend commented on your photo” e-mail: The e-mail is coming from a Gmail address — a fact that should tell the recipients that the e-mail is not legitimate. And, if they run their mouse over the embedded link, they will also notice that the real link has nothing to do with Facebook. A click on it will redirect the user to a malicious page serving malware. Source: [http://www.net-security.org/malware\\_news.php?id=1549](http://www.net-security.org/malware_news.php?id=1549)

## **NATIONAL MONUMENTS AND ICONS**

**(District of Columbia) New security planned for Washington Monument.** The National Park Service (NPS) is planning to upgrade the security facility at the Washington Monument in Washington D.C. to make the area more secure for visitors. Visitors to the Washington Monument have experienced enhanced security since the September 11 terrorist attacks, but a plywood trailer at the base of the monument will be replaced by a newly designed security center. The NPS has created four different plans for how pathways could lead visitors to a new underground facility, and the public can comment on the project plans until January 7. “The function of the underground screening security center is to provide an appropriate center that will allow us to maintain openness but also provide sufficient security so that people can use the monument,” a U.S. Park Police sergeant said. Source: <http://media.www.gwhatchet.com/media/storage/paper332/news/2010/12/02/News/New-Security.Planned.For.Washington.Monument-3963653.shtml>

UNCLASSIFIED

## UNCLASSIFIED

**(Missouri) Copper thieves hit historic KC park.** Thieves looking for copper have caused costly damage to a historic Kansas City, Missouri landmark, officials said. City officials said thieves caused \$80,000 in damage when they stripped copper from the domes along the colonnade at Kessler Park near Gladstone Boulevard and St. John Avenue in the old Northeast area of the city. The copper was installed in November 2004 during a restoration of the 100-year-old domes. City officials said crews will repair the damage over the winter, but they will use a material other than copper. The city has also installed security cameras at the park. Source: <http://www.fox4kc.com/news/wdaf-story-kessler-park-copper-theft-113010,0,10507.story>

### **POSTAL AND SHIPPING**

**(New York; New Jersey) Powder may have originated from N.Y.** FBI agents believe they closed the case of the white powder found in Park Ridge, Illinois October 4 with the apprehension of a woman in Ridgewood, New York. The 61-year-old suspect was taken into custody at her home October 28. According to documents released by the U.S. Attorney in the Eastern District of New York, the suspect, a retired elementary school teacher, allegedly sent dozens of powder-laced letters to former coworkers at P.S. 91 in Glendale, New York, as well as neighbors, and family members. The letters were sent during September and October. The U.S. Attorney did not specify what charges are currently placed against the suspect. Although the complaint does not specifically list the Park Ridge incident, a spokesperson from the FBI's New York office said the bureau believes the suspect was the sender of the letter to the Passionist Monastery. Source: <http://www.journal-topics.com/pr/10/pr101201.1.html>

**(Tennessee) Missing radioactive rods found by FedEx.** A shipment of radioactive rods that went missing Thanksgiving Day was found November 26 in Tennessee by the shipping company FedEx. Though the materials, used for medical equipment, posed little threat to the public, the misplaced shipment underscores the need to track low-hazard materials that could be used in small-scale terrorist attacks, experts said. The rods, used to calibrate quality control in CT scans, contain little energy and a low concentration of radiation, according to a FedEx spokeswoman. The shipment was sent from Fargo, North Dakota, and was reported missing at its destination in Knoxville, Tennessee. FedEx alerted all of its U.S. stations about the missing shipment. The shipment was found at a FedEx station in Knoxville, with its shipping label missing from the outer box, the spokeswoman said. All of the rods were intact and no FedEx employees were exposed to radiation. Three shipments of radioactive rods were mailed earlier this week. The recipient notified FedEx when only two containers arrived in Knoxville, the spokeswoman said. Source: <http://articles.latimes.com/2010/nov/27/nation/la-na-fedex-radiation-20101127>

### **PUBLIC HEALTH**

**(California) Newest whooping cough cases announced.** As the statewide whooping cough epidemic continues, health officials reported fewer new cases — a total of nine — the week of November 29 in San Diego County, California, that may have exposed other children to the highly contagious disease. Still, health officials urge families to make sure immunizations are up-to-date to protect the most vulnerable. Of the 41 people hospitalized in San Diego County for the disease this year, 30 were infants under the age of 1, five were children ages 1-18, and six were adults, according to the county health and human services agency. Two infants have died in San Diego out of 10 infant deaths

UNCLASSIFIED

## UNCLASSIFIED

statewide due to whooping cough, also known as pertussis. As of the week of November 29, there have been 960 cases of pertussis in the county, and 7,297 throughout California in the worst epidemic in 63 years, health officials said. Source:

<http://www.signonsandiego.com/news/2010/dec/01/newest-whooping-cough-cases-announced/>

**(Maryland) Md. fire marshal: Medical clinic blaze suspicious.** Maryland fire investigators said a blaze that destroyed a medical clinic in a historic Frederick, Maryland, farmhouse is considered suspicious. A deputy state fire marshal said November 26 that an arson dog detected accelerants at the scene of the November 25 fire in the farmhouse in the 8100 block of Runnymede Drive. Officials said two firefighters sustained minor injuries while battling the blaze. The marshal said investigators have been in touch with the owner, but he is out of the state. The clinic closed earlier this year after the doctor's medical license was suspended. Source: <http://www.myfoxdc.com/dpp/news/maryland/md-fire-marshal-medical-clinic-blaze-suspicious-112610>

**J&J recalls more Tylenol.** Johnson & Johnson (J&J) said November 24 it is recalling 9 million more bottles of its Tylenol painkiller because they do not adequately warn customers about the presence of trace amounts of alcohol used in the product flavorings. The latest in a string of J&J recalls involves three brands of Tylenol Cold Multi-Symptom Liquid. The Tylenol formulations include Daytime 8-ounce Citrus Burst, Severe 8-Ounce Cool Burst, and Nighttime 8-Ounce Cool Burst. "There is less than 1 percent alcohol in the flavoring, and this information is on the back of the bottles," a company spokeswoman said. "But the information does not appear on the front of the bottles," she added. More than 200 million packages of painkillers Tylenol and Motrin, allergy treatment Benadryl, and other consumer brands have been recalled over the past year due to quality-control lapses. The company said no side effects have been seen with the newly recalled liquid Tylenol products. Just days ago, J&J recalled almost 5 million packages of Benadryl, Motrin, and its Roloids antacid because of manufacturing "insufficiencies." J&J said those recalls, like many of the earlier ones, involved products made at its plant in Fort Washington, Pennsylvania. The facility was closed earlier this year to fix quality-control lapses, including unsanitary conditions, and is not expected to resume operations until late next year. Source: <http://www.reuters.com/article/idUSTRE6AN4WX20101124>

**Shortage of on-call trauma surgeons in U.S. hospitals: poll.** Three-quarters of U.S. emergency department directors said they do not have adequate on-call trauma surgeon coverage, and nearly one-quarter said their hospital's trauma center designation has been downgraded or lost, a new survey finds. The poll also found that: 60 percent of directors said their emergency department lost the ability to provide 24-hour coverage for at least one medical specialty in the last 4 years; more than 75 percent said their departments have inadequate coverage for plastic surgery, hand surgery, and neurosurgery; nearly 25 percent reported an increase in the number of patients leaving before being seen by a needed specialist, a situation that can lead to worse outcomes and increased need for hospitalization; inadequate surgical coverage was reported by 68 percent of teaching hospitals and 78 percent of non-teaching hospitals. The findings are published online and in the December print issue of the journal Academic Emergency Medicine. Source: <http://health.usnews.com/health-news/family-health/brain-and-behavior/articles/2010/11/29/shortage-of-on-call-trauma-surgeons-in-us-hospitals-poll.html>

UNCLASSIFIED

## **TRANSPORTATION**

**Amtrak lifts ban on guns.** Amtrak will let passengers transport unloaded guns on trains, reversing a ban in place since the September 11th terrorist attacks. The ban lifts December 15. Travelers can check firearms — including handguns, starter pistols, rifles, and shotguns — and up to 11 pounds of ammunition at any train station that offers checked baggage service and if the travelers' itinerary includes a train with a baggage car. Most big-city train stations — including New York, Boston, Chicago, and Washington D.C. — have checked-baggage service. Source:

[http://travel.usatoday.com/news/2010-11-30-amtrak-trains-guns\\_N.htm](http://travel.usatoday.com/news/2010-11-30-amtrak-trains-guns_N.htm)

**(New York) MTA terror-proofed tunnels nearly complete.** The Metropolitan Transit Authority (MTA) is nearing completion on a \$250 million anti-terror project to reinforce underwater subway tunnels and bridges in New York City against a bomb blast. Since 2004, agency contractors have been lining subway tubes — especially the 10 that run under the East River — with high-impact-bearing metal that would prevent collapse or massive flooding in the case of a terrorist attack. And in the more shallow tunnels that are not fully dug into rock, workers dropped massive slabs of rock and concrete on the riverbed to prevent disaster. The Post revealed November 30 how the Port Authority is paying \$600 million to beef up the vulnerable PATH subway tunnels beneath the Hudson River with blast plates and floodgates that would withstand rushing water in the case of an explosion. The agency's seven bridges are being "hardened" with plates and "collars" on cables that can resist a blast. In January, the state comptroller reported that "93 percent of all facility hardening was completed," and that the MTA's project cost about \$22 million more than expected. The MTA's security program also includes an increased police presence, and the "If You See Something, Say Something" campaign.

Source:

[http://www.nypost.com/p/news/local/mta\\_terror\\_proofs\\_bridges\\_tunnels\\_q4CYUqpXgQOXIP7jI3GGQj](http://www.nypost.com/p/news/local/mta_terror_proofs_bridges_tunnels_q4CYUqpXgQOXIP7jI3GGQj)

**May be time for tains, ships and mass transit to use body scanners, Napolitano says.** The Homeland Security Secretary hinted the week of November 22 that the body scanners and "enhanced" pat-downs that have caused a ruckus at airports across the country could be coming to a train stations, ports, or subways. In an interview on "Charlie Rose" that aired November 22, the Secretary said terrorists will continue to seek vulnerabilities in the nation's transportation systems. "I think the tighter we get on aviation, we have to also be thinking now about going on to mass transit or to trains or maritime," she said. "So what do we need to be doing to strengthen our protections there?"

Source: <http://www.infowars.com/may-be-time-for-trains-ships-and-mass-transit-to-use-body-scanners-napolitano-says/>

## **WATER AND DAMS**

**How will the power from the Klamath dams be replaced if they are removed?** There are a number of things concerning the proposed removal of four dams along the Klamath River in Oregon under the Klamath Hydroelectric Settlement Agreement (KHSA). Producing approximately 700,000 to 800,000 megawatt hours each year, the Klamath Hydroelectric Project provides enough power to serve 70,000 homes, according to dam owner PacifiCorp spokesman. The KHSA lays out the potential removal of four of the dams in the hydroelectric project, the power from which comprises about 2

## UNCLASSIFIED

percent of PacifiCorp's total generation capacity across its six-state range, according to an economic modeling report prepared for the California Energy Commission (CEC) in 2005 by the consulting firm M. Cubed. If the dams are removed in 2020, which is the projected earliest date for removal, PacifiCorp will look to replace the lost power from those facilities. While the decisions for replacing the power have not yet been announced, the M. Cubed report states the total costs for replacement power over a 30-year period are estimated in 2005 dollars to range from \$74 million to \$167 million, numbers that assume that replacement power will be at the decreased level expected under the relicensing scenario. If the dams are removed, PacifiCorp must turn to the Public Utilities Commissions in the states it serves in order to establish rates its customers will pay to cover the costs of replacing the lost power production. Source: <http://www.siskiyoudaily.com/features/x556838522/How-will-the-power-from-the-Klamath-dams-be-replaced-if-they-are-removed>

**(Tennessee) Rural streams contaminated.** Over 10,000 miles of streams have elevated contaminant levels in Tennessee, according to state officials. According to the biannual Status of Water Quality in Tennessee report issued in November by the Tennessee Department of Environment and Conservation Division of Water Pollution Control, 67 percent of the miles of streams designated for fish and aquatic-life protection meet federal Environmental Protection Agency standards, and only 57 percent of the miles of streams designated for recreation were found to meet the federal standards. While Tennessee's drinking water is relatively safe, a spokesperson stated, pollution in other parts of the water table could have an effect on drinking water. The three biggest factors negatively impacting Tennessee's streams are bacteria, silt and an over-abundance of vital nutrients, a spokesperson stated, adding that land-use issues are a leading cause in elevating all of these factors. One big cause of all three of these factors, a spokesperson stated, is agriculture. Clearing out brush or forests to develop fields or pastures reduces the buffer that protects streams from pollutants and silt runoff, and livestock that have open access to running water can contaminate streams with waste, a spokesperson stated, adding that fertilizers can introduce an overabundance of nutrients into the water table. Source: <http://www.mtsusidelines.com/news/rural-streams-contaminated-1.1816323>

## **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](mailto: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](mailto:kihagel@nd.gov), 701-328-8168



UNCLASSIFIED

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**