



# Homeland Security

## Daily Open Source Infrastructure Report for 11 February 2010

**Current Nationwide Threat Level**

**ELEVATED**

**Significant Risk of Terrorist Attacks**

For information, click here:  
<http://www.dhs.gov>

### Top Stories

- Bloomberg reports that blizzard warnings were posted from Washington to Long Island, closing government offices, grounding 9 percent of U.S. flights, and forcing the closure of Interstates 83, 78, 77, 476, 176, 676, and parts of 81 in Pennsylvania. “It may take days for the infrastructure associated within [the Washington-Philadelphia-New York urban corridor] to fully recover,” said an energy meteorologist at Planalytics Inc. (See item [23](#))
- According to the Associated Press, a former U.S. Army computer-security specialist has found a way to break into a chip that carries a “Trusted Platform Module” designation, billed as among the industry’s most secure. (See item [43](#))

### Fast Jump Menu

#### PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

#### SUSTENANCE AND HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

#### SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

#### FEDERAL AND STATE

- [Government Facilities](#)
- [Emergency Services](#)
- [National Monuments and Icons](#)

### Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *February 8, WSBT 22 South Bend* – (Indiana) **Highway re-opens after fuel spill at Elkhart railyard.** Authorities have re-opened U.S. 33 in Elkhart, after cleaning up a fuel spill late Sunday at the Norfolk Southern railyard. An estimated 200 gallons of

fuel had spilled from a station at the yards at old U.S. 33, just west of Indiana 19. Old U.S. 33 was closed in the area near the Franklin Street intersection while crews worked to remove the fuel.

Source: <http://www.wsbt.com/news/local/83779342.html>

2. *February 7, Ledger* – (Florida) **Many gas storage tanks in Polk in need of upgrades.** Owners of 165 underground gas storage tanks at 51 sites around Polk County have failed to upgrade the tanks as required by a 1983 state law, according to state officials. The law, one of the first in the nation, was designed to reduce the risk of groundwater contamination. Tank owners had until December 31 to upgrade their tank systems to install double containment walls that will prevent contamination from spreading even if a tank leaks. The rules have been in effect since 1991, according to the Florida Department of Environmental Protection (DEP), which sent notices to tank owners in August 2009 reminding them of the deadline. Tank owners who missed the deadline have three options, according to a DEP spokeswoman: Apply for a three-month extension if they have a contract in place to have the work performed. Remain in business as long as the tanks are taken out of service or are permanently closed. Ask for a further time extension by entering into a consent order, which will set a specific deadline to comply. “(DEP) may pursue action in Circuit Court against facility owners who continue to operate non-compliant facilities (failure to meet upgrade deadline) absent any of the provisions listed above,” she said. She said the agency can also seek injunctive relief to require tank closure and to assess fines. “Each enforcement case is handled on a case-by-case basis,” she said. Unlike the cleanup of sites contaminated by leaking tanks, which is funded in part by a state trust fund, the cost of upgrading facilities is the responsibility of the tank’s owner, she said.

Source:

<http://www.theledger.com/article/20100207/NEWS/2075032/1410?Title=Many-Gas-Storage-Tanks-in-Polk-in-Need-of-Upgrades&tc=ar>

For another story, see item [23](#)

[\[Return to top\]](#)

## **Chemical Industry Sector**

3. *February 9, Daily News Online* – (Washington) **Sensors failed to identify Weyerhaeuser chlorine leak.** An open valve at Weyerhaeuser Co.’s pulp mill in Longview sent 137 pounds of chlorine gas into the air undetected over the several days, but company officials said the leak is fixed. Workers discovered the leak on February 8 while testing why a piece of equipment in the mill’s fiber line was not working, a Weyerhaeuser spokesman said. The workers immediately closed the valve and stopped the leak, he said. The leak failed to trigger the mill’s chlorine gas detection alarms because the concentration of gas was too low, he said. County emergency management officials say they received no calls about the leak, and Weyerhaeuser received no complaints on its 24-hour hotline. Weyerhaeuser uses chlorine to bleach the wood pulp to make white or light-colored paper products. State Department of Ecology officials cannot determine the health danger of the chlorine

leak without knowing how many days it lasted, an agency spokeswoman said on February 9. Ecology plans to look into the release further, she said. Weyerhaeuser officials alerted state and county emergency management officials and the National Response Center — the agency that records chemical spills and emissions — as soon as they discovered the leak. The company is conducting an internal investigation to determine what went wrong, he said. “We’ll do everything we can to prevent this from happening in the future,” he said.

Source: [http://www.tdn.com/news/local/article\\_48be9bd2-15e4-11df-9630-001cc4c03286.html](http://www.tdn.com/news/local/article_48be9bd2-15e4-11df-9630-001cc4c03286.html)

4. *February 9, San Antonio Express-News* – (Texas) **Better hazmat plan for fires sought.** More than three years after a huge mulch fire threatened to pollute San Antonio’s water supply, the Edwards Aquifer Authority (EAA) is considering new rules for the storage of chemicals above the aquifer’s recharge zone. The December 2006 mulch fire in Helotes tainted wells with ash runoff and made aquifer managers realize the water supply was vulnerable to similar threats. “Some of the wells were like you had washed out your barbecue pit,” said the assistant general manager at the Edwards Aquifer Authority. Fortunately, the runoff was not toxic, but the authority is concerned the next major fire will not be of decomposing brush, but at a warehouse full of pesticides and solvents like those stored and sold at major retail stores. If one of those buildings were to start burning and then become doused by firefighters, the runoff could carry those toxic chemicals directly into the aquifer. The authority has identified 28 businesses in the aquifer recharge zone that could be affected by the new rules. They include big-box stores, quarries, paint companies and county and city buildings, any place that stores large quantities of motor oil, antifreeze, pesticides and other potentially hazardous chemicals. Starting this week, the authority will host a series of public meetings to gather input on new rules designed to protect the aquifer by requiring all property owners storing more than 10,000 pounds or 1,000 gallons of “regulated substances” to notify the authority of where the material is, what the plan is if the material is threatened by a fire, and where the containment equipment and safety equipment is kept. The information will be stored in an online database so firefighters responding to a call will know how to best address the situation. In some cases, the information may tell the firefighters to simply let the fire burn itself out. Every fire is different, and the new rules will give firefighters more information on which to base their decision, explained an EAA spokesman.

Source: <http://www.mysanantonio.com/livinggreensa/83856487.html>

5. *February 8, Tennessean* – (Tennessee) **Two Franklin factories face fines from EPA.** U.S. Environmental Protection Agency (EPA) has fined two Franklin manufacturers more than \$56,000 for years of not filling federal documentation about the amounts of hazardous chemicals they have at their plants. The agency fined metal home products maker Lasko Products \$29,559 and paint-maker Egyptian Lacquer Manufacturing Co. Inc. \$27,183 separately after inspections in December turned up years of instances where the companies did not properly list quantities of chemicals they had at their facilities. According to the EPA’s letters, Lasko had quantities of sulfuric acid, enamel and poly propylene pellets above their previously reported limits for 2006, 2007 and

2008. Egyptian Lacquer did not list the chemical toluene and 27 other chemicals above the company's reported limits for 2004, 2005 and 2006. Local emergency responders use the information on companies' Tier I and Tier II forms to plan in case potential emergencies at those facilities were to occur.

Source:

<http://www.tennessean.com/article/20100208/WILLIAMSON01/100208043/Two+Franklin+factories+face+finer+from+EPA>

[\[Return to top\]](#)

## **Nuclear Reactors, Materials, and Waste Sector**

6. *February 9, WYFF 4 Greenville* – (South Carolina) **Wells near nuclear plant fail test.** Two groundwater monitoring wells at Oconee Nuclear Station indicate that groundwater has exceeded the nuclear industry's voluntary reporting level for tritium, a byproduct of reactor operations. The level of tritium exceeds the Environmental Protection Agency (EPA) standard for public drinking supply, but the wells are not part of the plant's drinking water system, officials said. "The samples were taken from two monitoring wells, not drinking water wells. There is no health risk to the public or plant employees or a violation of EPA standards since this water is not for consumption," said the Oconee site vice president. "These monitoring wells are located on the site property near the main plant buildings. Other well samples show these tritium levels are confined to the plant property."  
Source: <http://www.wyff4.com/news/22513732/detail.html>
7. *February 9, Mid-Columbia Tri-City Herald* – (Washington) **Richland nuclear fuel lab fire put out quickly.** A very small fire in a laboratory at Areva NP in Richland was quickly extinguished by a lab worker Monday afternoon. The manager of environmental health, safety and licensing at the plant characterized the fire's size as "a handful of flames." Areva believes that some fine shavings of the flammable metal zirconium caught fire. No radiological materials were in the part of the lab where the fire occurred. The laboratory is used to test metal samples for quality and material characteristics. Metals may be polished, and fine shavings can result. The Areva emergency management response team assembled and the Richland Fire Department responded, but neither was needed. Areva produces fuel for nuclear power plants.  
Source: [http://www.tri-cityherald.com/kennewick\\_pasco\\_richland/story/894784.html](http://www.tri-cityherald.com/kennewick_pasco_richland/story/894784.html)
8. *February 9, Huntsville Times* – (Alabama) **Environmental group cites potential radiation risks in opposing Bellefonte nuclear project.** A North Carolina environmental group is seeking to sway local officials from supporting completion of Tennessee Valley Authority's (TVA) Bellefonte Nuclear Plant near Scottsboro, Alabama, or the construction of a new nuclear plant next to it. "We don't want to see mistakes repeated here," the science director for the Blue Ridge Environmental Defense League told the Scottsboro City Council Monday, referring to the 1979 accident at Three Mile Island nuclear plant near Harrisburg, Pennsylvania. But the vice president of Nuclear Generation Development at TVA said in an interview

Tuesday the public will have “nothing to fear” if a nuclear plant becomes operational at Bellefonte. The TVA Board of Directors is expected to decide April 16 whether to finish one of Bellefonte’s two units, build a new unit, or take no action. The City Council is expected to adopt a resolution supporting the Bellefonte project. The science director and others in his group said they oppose the plant because of the cost of construction and the potential for radioactive leaks.

Source: [http://blog.al.com/breaking/2010/02/environmental\\_group\\_cites\\_pote.html](http://blog.al.com/breaking/2010/02/environmental_group_cites_pote.html)

9. *February 9, Las Vegas Sun* – (Nevada) **Feds seeking withdrawal of Yucca Mountain water applications.** The Yucca Mountain Nuclear Waste Repository got another nail in its coffin today, as the Energy Department formally asked to withdraw its applications for access to water in the area surrounding Yucca Mountain. The request came after the state engineer twice wrote to the agency to ask whether he should continue with the application, given the President’s stated plan to kill the planned nuclear waste dump. The Energy Department had sought 116 different water rights for the Yucca Mountain project, but the exact amount of groundwater in question was not immediately available from the state Division of Water Resources. The Energy Department has stated it plans to submit a motion to withdraw the Yucca Mountain Waste Repository license application and that it intends never to revive the project.

Source: <http://www.lasvegassun.com/news/2010/feb/09/feds-seek-withdrawal-yucca-mountain-water-applicat/>

For another story, see item [32](#)

[\[Return to top\]](#)

## **Critical Manufacturing Sector**

10. *February 9, Glens Falls Post-Star* – (New York) **Firefighters exposed to chemicals during mill fire.** A Glens Falls, New York, firefighter was treated at Glens Falls Hospital for chemical exposure and several other suffered exposure to a chemical after a smoky fire at a Rogers Street mill on Monday afternoon. The firefighters were exposed to silver nitrate, a chemical that is used in the battery manufacturing process that causes the skin to be stained black, during the fire at Ames Goldsmith, officials said. Several firefighters got the substance on their faces and hands, but they are not expected to have any lasting health problems from it, said the Glens Falls interim Fire Chief. It turns the skin black for a period of days, but when treated with soap and lotion the skin will return to normal. The chemical got on their skin through gaps in their turnout gear, said an assistant fire chief. The fire broke out about 2:30 p.m. in a machine that dries silver nitrate to crystallize it. It appears the machine overheated, which caused oil from inside the machine to drip into the silver nitrate and the chemical to ignite. The fire spread from the drying machine to adjacent equipment, and caused extensive damage to the dryer. Ames Goldsmith officials said Monday that the plant would remain open but that the dryer would need repairs.

Source: [http://www.poststar.com/news/local/article\\_39d8ea26-15b4-11df-a69d-](http://www.poststar.com/news/local/article_39d8ea26-15b4-11df-a69d-)

[001cc4c03286.html](http://001cc4c03286.html)

11. *February 9, Wausau Daily Herald* – (Wisconsin) **Man in critical condition after industrial explosion.** A 31-year-old man was in critical condition Tuesday at the University of Wisconsin Hospital and Clinics Burn Center in Madison, according to a hospital spokesperson after an industrial accident at a Schofield business. The Schofield Fire Department was called to Quality Surface Processing for a report of an explosion. Employees at the business were stripping paint from pieces of metal by putting the metal in a salt bath when a chemical reaction occurred, the police said. Temperatures in the salt bath approach 900 degrees, he said. The man was burned as a result of the chemical reaction. Two others were treated at the scene for inhalation of smoke or chemicals, the police said. A small fire started as a result of the chemical reaction, but was quickly extinguished. Firefighters used fans to vent smoke and fumes from inside the building.

Source:

<http://www.wausaudailyherald.com/article/20100209/WDH0101/100209045/Updated-Man-in-critical-condition-after-industrial-explosion>

12. *February 9, Rockford Register-Star* – (Illinois) **One man injured in industrial plant fire in Oregon.** One man was injured late Tuesday afternoon in an industrial plant fire at HA International. The fire was reported about 5 p.m. The injured person is believed to be one of 15 employees inside the plant when the fire started. The extent of his injuries was not known. An Ogle County sheriff's official said the fire started on the roof of the plant when a motor overheated. The official cause and damage amount was not available late Tuesday night. HA International is a multipurpose plant offering painting services, web coating services, plating services, electro coating services, as well as heat treatment services, welding and brazing and soldering services.

Source: <http://www.rrstar.com/news/x1328931490/One-man-injured-in-industrial-plant-fire>

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

13. *February 10, Associated Press* – (North Dakota) **Software glitch grounds border security drones.** The former Director of the Homeland Security unmanned aerial vehicle program at Grand Forks air force base says a software glitch grounded the two Predator B drones used for northern border patrol. He says that during a flight in early November the remotely piloted aircraft did not respond properly after the communication link with the base center was lost. He says there was no serious safety or security issue and nothing was damaged, but some of the software language in the program will need to be changed. He directed Homeland Security's UAS operations at the base from 2007 until he resigned January 2 to take a job with a Fargo engineering firm. His replacement did not immediately comment on the software problem but said border security has not been compromised because manned helicopters and planes also are used.

Source: [http://www.kfgo.com/regionalnews\\_Detail.php?ID=11215](http://www.kfgo.com/regionalnews_Detail.php?ID=11215)

14. *February 9, Popular Science* – (National) **Marine Corps' unmanned programmable copter passes first major test.** The difficulty of supplying remote outposts across rugged terrain has contributed to many of the deadliest moments in the Afghan War, by preventing the delivery of weapons and ammo to engaged soldiers, forcing supplies to travel over dangerous roads, or turning helicopters into vulnerable targets. Last June, the Marines put out a call for a helicopter UAV to solve those problems. Now, with a successful demonstration at Utah's Dugway Proving Grounds, the Marines might have found their robocopter. In the demonstration, a modified K-MAX helicopter moved 3,000 pounds across 600 miles, in under six hours. The K-MAX, built by Kamen Aerospace, is a single-seat helicopter designed specifically to carry cargo externally slung beneath the craft. For the Marines, Kamen simply removed the crew cabin, and transformed the helicopter into a UAV. The UAV performed the mission with almost no hands-on control. A ground operator only adjusted the flight path at the request of Marine observers who wanted to see what the chopper could do. Otherwise, the UAV flew the entire mission on programming.  
Source: <http://www.popsci.com/technology/article/2010-02/copter-uav-passes-marine-corps-cargo-haul-test>
15. *February 8, Go Erie* – (Pennsylvania) **Firefighters respond to smoke at Erie plant.** Fire crews responded to reports of smoke at an Erie manufacturing plant earlier Monday morning. Smoke filled a room at Composiflex Inc., after an employee turned on the heat. The Perry Hi-Way Hose Co. chief said a heater motor burned out. Crews were able to contain the smoke to one room, she said. Only a few employees were inside the building at the time, and no one was injured.  
Source:  
<http://www.goerie.com/apps/pbcs.dll/article?AID=/20100208/NEWS02/302089922>

For another story, see item [42](#)

[\[Return to top\]](#)

## **Banking and Finance Sector**

16. *February 10, McHenry County Northwest Herald* – (Illinois) **Bomb threat made at bank.** The Chicago FBI and Wauconda Police Department are investigating an attempted robbery that happened on February 9 at Wauconda Community Bank. According to initial reports, a lone male entered the bank and placed a package on a counter. He then turned and walked away. A note attached to the package claimed that a bomb was inside and instructed employees to place an unspecified amount of cash at a nearby location or the bomb would be detonated. The robbery attempt was unsuccessful, as no money was removed from the bank, according to an FBI news release. The bank and surrounding area were evacuated. No explosives were found inside the package, and no injuries were reported.  
Source:  
[http://www.nwherald.com/articles/2010/02/10/r\\_y0abjwb2toi6\\_f\\_wwjblya/index.xml](http://www.nwherald.com/articles/2010/02/10/r_y0abjwb2toi6_f_wwjblya/index.xml)

17. *February 10, LawyersandSettlements.com* – (National) **iPhone users committing insurance fraud to get newest models.** Apple has generated enormous customer loyalty with its line of computers and personal electronics. However, a recent report claims that many users of the company’s immensely popular iPhone may routinely commit insurance fraud in the hopes of picking up the newer, faster models. A director at Supercover Insurance claims that the number of lost, stolen or damaged phone complaints grows exponentially every time Apple launches a new generation of smartphone technology. Many service plans for the popular gadget allow the consumer to receive a replacement phone in the event of theft or irreparable damage — and those replacements are usually the latest model of the phone. Supercover tells PCR Magazine that iPhone owners are 60 percent more likely to take out insurance on their phone than users of any other brand. “While most customers take out insurance because they value their iPhone, we started to notice increases in claims as new and upgraded iPhones were launched — for short periods around new model or upgrade launches, claims for lost, stolen or damaged iPhones go through the roof,” the director told the magazine.  
Source: <http://www.lawyersandsettlements.com/articles/13564/insurance-law-bad-faith-claim.html>
18. *February 9, Computerworld* – (International) **New Russian botnet tries to kill rival.** An upstart Trojan horse program has decided to take on its much-larger rival by stealing data and then removing the malicious program from infected computers. Security researchers say that the relatively unknown added this functionality just a few days ago in a bid to displace its larger rival, known as Zeus. The feature, called “Kill Zeus,” apparently removes the Zeus software from the victim’s PC, giving Spy Eye exclusive access to usernames and passwords. Zeus and Spy Eye are both Trojan-making toolkits, designed to give criminals an easy way to set up their own “botnet” networks of password-stealing programs. These programs emerged as a major problem in 2009, with the U.S. Federal Bureau of Investigation estimating last October that they have caused \$100 million in losses. Trojans such as Zeus and Spy Eye steal online banking credentials. This information is then used to empty bank accounts by transferring funds to so-called money mules — U.S. residents with bank accounts — who then move the cash out of the country. Sensing an opportunity, a number of similar Trojans have emerged recently, including Filon, Clod and [Bugat], which was discovered just last month.  
Source:  
[http://www.computerworld.com/s/article/9154618/New\\_Russian\\_botnet\\_tries\\_to\\_kill\\_rival](http://www.computerworld.com/s/article/9154618/New_Russian_botnet_tries_to_kill_rival)
19. *February 9, DarkReading* – (International) **New banking trojan discovered targeting businesses’ financial accounts.** The infamous Zbot botnet that spreads the pervasive Zeus Trojan has been seen distributing a brand-new banking Trojan — one that researchers say could serve as a lower-cost alternative to the popular Zeus and Clampi malware for cybercriminals. The new Bugat Trojan, which was discovered by researchers at SecureWorks, appears to be aimed at mostly business customers of large and midsize banks. It is built for attacks that hack automated clearinghouse (ACH) and

wire transfer transactions for check and payment processing — attacks in which U.S.-based SMBs and state and local governments are losing an average of \$100,000 to \$200,000 per day, according to data from Neustar. To date, Zeus and Clampi Trojans have mostly been used for stealing financial credentials. But a security researcher with SecureWorks' Counter Threat Unit (CTU) says Bugat has some of the same features as other banking Trojans, but with a few twists: It uses an SSL-encrypted command and control (C&C) infrastructure via HTTP-S, and also goes after FTP and POP credentials via those encrypted sessions. The researcher says SecureWorks has witnessed around 1,200 to 3,000 Bogat attack attempts during the past week against its clients. "We saw in the wild that it was being distributed from a specific Zeus botnet," he says. "Oddly enough, its purpose is the same as Zeus ... but it's something not as recognizable as Zeus or that's cheaper [to purchase] in the long term." Bugat's main targets so far are business financial accounts.

Source:

[http://www.darkreading.com/vulnerability\\_management/security/client/showArticle.jhtml?articleID=222700615&subSection=End+user/client+security](http://www.darkreading.com/vulnerability_management/security/client/showArticle.jhtml?articleID=222700615&subSection=End+user/client+security)

20. *February 9, NewsFactor* – (National) **Red Condor warns of trending phishing campaign.** Old is new again for scammers as spam emails targeting attorneys are once again on the rise. Email security experts at Red Condor have issued a warning for trending phishing attacks requesting legal representation to help in the "collection of delinquent accounts." The majority of the messages with subject lines, including "Attn: Legal Counsel," "Dear Attorney," and "Legal Assistance," appear to come from legitimate corporations from the Asia-Pacific region such as Nabtesco Corporation, Nippon Steel Corporation, South China Industrial Company and Turfchem Sdn. Bhd. Recent campaigns have also claimed to be from a London organization. But the emails actually originate from servers around the world, including Canada, Germany, Malaysia, Nigeria and the U.K. with a web mail sender address such as Yahoo.

Source: [http://www.newsfactor.com/news/Red-Condor-Warns-of-Phishing-Scam/story.xhtml?story\\_id=021000D80430](http://www.newsfactor.com/news/Red-Condor-Warns-of-Phishing-Scam/story.xhtml?story_id=021000D80430)

21. *February 9, NBC New York* – (New York) **FBI hunts Queens bank robbers who use gun, fake bomb.** Armed with a handgun and a fake bomb, two men have robbed four banks in Queens in the last two weeks. Nobody has been hurt in the hold-ups. But FBI and NYPD officials are worried it is only a matter of time before they hurt someone if they are not caught. This bank robbery spree began back on January 22 with a hold-up of the Queens County Savings bank on Jamaica Avenue. Another nearby branch was robbed just three days later. Then the suspects hit Chase banks along Northern Boulevard and Horace Harding Boulevard. Investigators said the pair has made off with tens of thousands of dollars so far. In each case, one of the suspects enters the bank with the gun and a device made up of two flares. The other suspect waits outside as a lookout. The suspects have worn dark long coats and hats during the robberies.

Source: <http://www.nbcnewyork.com/news/local-beat/Queens-Bank-Robbers-Using-Gun-and-Fake-Bomb-83966327.html>

22. *February 9, Associated Press* – (Georgia) **Man charged with manufacturing fake Treasury bonds.** A Duluth man has been charged with manufacturing more than \$1.6 billion in fraudulent U.S. Treasury bonds and other government documents. Gwinnett County sheriff’s investigators say they learned on February 1 that the suspect wanted to purchase a home by using a registered promissory note supposedly certified by the U.S. Treasury Secretary. A Gwinnett police corporal says an attorney who received the note realized it was fake and notified police. On February 4, the suspect attended a loan closing at the attorney’s office, where the suspect presented the \$225,000 note for payment to purchase a home in Lawrenceville. Investigators confirmed that the suspect signed the loan documents under false pretense and he was arrested. The 57-year-old is charged with residential mortgage fraud.

Source:

[http://www2.wrbl.com/rbl/ap\\_exchange/georgia\\_news/article/ManChargedWithManufacturingFakeTreasuryBondsGa/129264/](http://www2.wrbl.com/rbl/ap_exchange/georgia_news/article/ManChargedWithManufacturingFakeTreasuryBondsGa/129264/)

[\[Return to top\]](#)

## **Transportation Sector**

23. *February 10, Bloomberg* – (National) **Blizzard scrubs flights, snarls eastern U.S. cities.** Blizzard warnings for as much as 20 inches of snow were posted from Washington to Long Island as a storm settled in for a daylong siege, closing government offices, grounding 9 percent of U.S. flights, and threatening 3 inches an hour for New York. Gusts of nearly 60 mph are expected from North Carolina to Massachusetts, which may knock down trees and power lines, causing widespread power disruptions, said the National Weather Service. “It may take days for the infrastructure associated within [the Washington-Philadelphia-New York urban corridor] to fully recover,” said a senior energy meteorologist at Planalytics Inc. New York-based Consolidated Edison Inc. is adding extra crews to help avert snow- and ice-related blackouts. Washington’s electric supplier Pepco pulled its crews off the streets because of unsafe conditions. The Pennsylvania Governor ordered Interstates 83, 78, 77, 476, 176, 676, and parts of 81 to close. New Jersey Transit said it would curtail its schedules after 2:30 p.m. Amtrak has not run a full schedule since last week’s storm and more trains were canceled Tuesday. More than 4,200 flights have been canceled in the United States so far Wednesday, or about 9 percent of the total schedule, according to FlightStats.com. More than 500 flights have been canceled for Thursday and “hundreds and hundreds more” are likely, said a FlightStats.com spokesperson. Washington’s Dulles and Reagan National airports were closed.

Source: <http://www.bloomberg.com/apps/news?pid=20601100&sid=aHolWt.lcwc0>

24. *February 10, Associated Press* – (National) **American Airlines-FAA.** Government and industry officials say the FAA is close to wrapping up a two-year investigation of safety violations at American Airlines. The result could be one of the largest fines in the agency’s history. The officials who spoke on condition of anonymity say the FAA investigation involves improperly secured wiring in 290 MD-80s. The wires could become damaged and, in some cases, presented a potential fire hazard. Hundreds of planes were grounded in April 2008 because of the problem. The officials say while

the amount of the fine has not yet been determined, it will likely be in the same ballpark as the more than \$10 million fine levied against Southwest for planes that missed required examinations. It was ultimately settled for \$7.5 million. Separately, the officials say the Transportation Department's inspector general is due to release an audit in the next several days that criticizes FAA for lax oversight of aircraft maintenance at American.

Source: [http://www.wlos.com/template/inews\\_wire/wires.national/2ad9a42f-www.wlos.com.shtml](http://www.wlos.com/template/inews_wire/wires.national/2ad9a42f-www.wlos.com.shtml)

25. *February 9, Aviation Web* – (National) **Delta aims to prevent crew overflights.** Dispatchers at Delta Air Lines will soon be able to contact flight crews with special sound alerts, rather than text messages only, to avoid an incident like the one last October when two distracted pilots overflew their destination by more than an hour, the airline has told the NTSB. In a document filed with the safety board, the airline said it is changing its software so dispatchers will be able to send aural alerts to Airbus A320 and A319 cockpits, in addition to text messages. The two pilots, who at the time were operating as a Northwest Airlines flight, told investigators they were at a loss to explain how they flew so far off course without noticing. The Air Line Pilots Association told the NTSB it would also be a good idea to consider installing “crew alertness monitors” on A320s that automatically sound an alert and trigger red flashing lights if the crew goes quiet for too long. The National Air Traffic Controllers Association agreed in its statement to the NTSB that an aural alert system would be a good idea. NATCA also suggested that controllers need to have current phone numbers for air carrier dispatch desks as well as refresher training on NORDDO procedures. The FAA has revoked the certificates of both pilots.

Source:

[http://www.avweb.com/avwebflash/news/DeltaChangesAimToPreventCrewOverflights\\_201989-1.html](http://www.avweb.com/avwebflash/news/DeltaChangesAimToPreventCrewOverflights_201989-1.html)

26. *February 9, Next Gov* – (National) **FAA asks for big increase for next-generation air traffic control system.** The White House asked for a dramatic increase for its ongoing program to replace the decades-old air traffic control system with a one that relies on GPS, real-time weather updates in cockpits and enhanced runway control. The U.S. President asked for a \$1.14 billion budget in fiscal 2011 for the FAA's Next-Generation Air Transportation System, a 31 percent increase from the \$867.7 million fiscal 2010 budget. The NexGen program incorporates more than two dozen projects that will transform the air traffic control system in the United States by 2025, FAA said in its budget request. NexGen will replace today's radar-based system, which relies on extensive voice communications between controllers and pilots, with a GPS satellite-based system. Current voice communications systems will not be able to manage the projected growth in air traffic after 2020 and data communications lies at the heart of its advanced airspace management system, the agency said. As part of the NextGen budget request, FAA asked for \$153.3 million for data communications in fiscal 2011, more than three times the \$46.7 million the agency spent in fiscal 2010. The amount was the largest increase in the fiscal 2011 NexGen budget. FAA plans to deploy data communications in phases, starting with automated clearances for takeoffs

and eventually managing enroute communications between pilots and controllers. The agency said the budget will support specification and standards development for data link services, systems engineering and integration.

Source: [http://www.nextgov.com/nextgov/ng\\_20100209\\_3651.php?oref=topnews](http://www.nextgov.com/nextgov/ng_20100209_3651.php?oref=topnews)

For more stories, see items [1](#) and [28](#)

[\[Return to top\]](#)

## **Postal and Shipping Sector**

27. *February 10, Fort Myers News-Press* – (Florida) **Donut powder leads to Pine Island hazmat scare.** Employees opening the mail at a doctor’s office in Matlacha, Florida, found white powder inside an envelope containing a check. They soon called 911 and sheriff’s deputies, a county hazardous materials team, and a nearby fire rescue truck rushed to the building. Meanwhile, the person who mailed the envelope was contacted by the doctor’s staff. “He said he was eating a powdered doughnut when he mailed the check,” said a sheriff’s spokeswoman. What might have been a menacing substance turned out to be nothing more than confectionary sugar, the spokeswoman said. The doctor did not return calls for comment. The spokeswoman said she could not fault the doctor’s staff. “With everything going on in the world today, you can’t be too careful,” she said.

Source: <http://www.news-press.com/article/20100210/NEWS0101/2100392/1003/ACC/Doughnut-powder-leads-to-Pine-Island-HAZMAT-scare>

[\[Return to top\]](#)

## **Agriculture and Food Sector**

28. *February 9, KansasCity.com* – (Missouri) **Semi-tractor trailers hauling soda, milk crash on I-29 near Dearborn.** All lanes of Interstate 29 near Dearborn have reopened after an early morning crash involving two semi-tractor trailers, according to the Missouri Highway Patrol (MHP). One semi spilled its load of soda on the interstate. The other truck, carrying milk, careened down an embankment, coming to rest in a creek bed about 50 feet off the roadway, according to MHP. The crash occurred about 5:15 a.m. near mile marker 31.6 in the southbound lanes of I-29. One of the drivers was driving southbound in a 2007 Kenworth tanker truck when he drove onto the shoulder and struck the trailer of a parked 2004 Peterbilt, according to MHP. The Kenworth truck continued down the side of the parked truck and then ran off the right side of the roadway, striking a guardrail. The truck continued down the embankment and overturned. The driver was ejected. He was taken to a hospital with moderate injuries. The driver of the Peterbilt truck was not injured. Neither of the drivers were wearing a seatbelt, according to MHP.

Source: [http://www.kansascity.com/116/story/1736288.html?storylink=omni\\_popular](http://www.kansascity.com/116/story/1736288.html?storylink=omni_popular)

29. *February 9, Associated Press* – (North Dakota) **Food warehouse roof in Fargo**

**collapses.** Authorities say snow and ice buildup led to roof collapses at a large food warehouse in Fargo. The fire department's captain said no one was hurt in the collapses late Monday and early Tuesday. He said a 100-by-100-foot section of the Sysco Food Service roof collapsed just after 10 p.m. Monday, breaking the sprinkler system and flooding parts of the building. Damage was estimated at about \$300,000. About 7 a.m. Tuesday, a 50-by-100-foot section broke off and plunged all the way to the floor. The collapse shut down operations at the warehouse, which serves clients in North Dakota, northwest Minnesota and northern South Dakota. A company official says Sysco is working to deliver products to those customers from Sysco Foods facilities in Minnesota, Montana and Nebraska.

Source: <http://www.wday.com/event/article/id/29742/>

30. *February 9, WPVI 6 Philadelphia* – (Pennsylvania) **Fire at Phila. Tastykake factory.** The fire happened in an oven around 11:25 a.m. at the factory in the 2900 block of West Hunting Park Avenue. When firefighters arrived, they found smoke coming from the third floor of the building resulting in a prompt evacuation of the building. They turned off all of the ovens and extinguished the fire. A second oven then caught fire, but that was quickly put out. There are no reported injuries.

Source: <http://abclocal.go.com/wpvi/story?section=news/local&id=7266925>

[\[Return to top\]](#)

## **Water Sector**

31. *February 10, Huron Daily Tribune* – (Michigan) **Alarm at Waste Water facility no cause for concern.** An alarm that sounded at approximately 3 a.m. on February 10 at the Waste Water Treatment Facility in Bad Axe, Michigan, was not an emergency, according to police. A Bad Axe City Police patrol officer said he responded to the alarm after residents called Central Dispatch. While he does not know at this time what caused the alarm to sound, he said there are no problems at the plant that will affect residents. The director of public works was not available for comment as of press time.

Source:

[http://www.michiganstumb.com/articles/2010/02/10/news/local\\_news/doc4b72a9e1ce447864323102.txt](http://www.michiganstumb.com/articles/2010/02/10/news/local_news/doc4b72a9e1ce447864323102.txt)

32. *February 9, Associated Press* – (Vermont) **Vt. Health chief: Tritium may be in Connecticut River.** Vermont's top health official said Tuesday it is reasonable to assume a radioactive substance leaking from the Vermont Yankee nuclear plant is reaching the Connecticut River. The commissioner of the state Department of Health told the Associated Press that the volume and direction of flow of tritium-tainted groundwater leads to the conclusion that it is reaching the river. Previous statements from the Health Department had indicated the water containing tritium, a radioactive isotope of hydrogen that has been linked to cancer when ingested in large amounts, was believed to be flowing toward or to the river. But they also said it was diluted by uncontaminated river water, so that lab instruments were not detecting it in samples of river water. The commissioner said Tuesday that continued to be the case because of

the river's rapid, heavy flow. "There's no indication at the moment with respect to either the river or all the other places we're monitoring that suggest people need to take any different actions, to do anything differently," the commissioner said. A Vermont Yankee spokesman said plant officials agreed with the commissioner's assessment that tritium is reaching the river.

Source:

[http://www.google.com/hostednews/ap/article/ALeqM5jo7gytGIVNSxu\\_MnfEbvaelD0zcQD9DP1ELO0](http://www.google.com/hostednews/ap/article/ALeqM5jo7gytGIVNSxu_MnfEbvaelD0zcQD9DP1ELO0)

33. *February 9, KMED 1440 Medford* – (Oregon) **Gravel from Savage Rapids recently opened are causing clog in Grants Pass Pumping Station.** The newly revealed Savage Rapids on the Rogue River need some fixing. Savage Rapids Dam was removed last fall, exposing the rapids. But the Medford Mail Tribune reports that material once trapped behind the dam is clogging the Grants Pass Irrigation District's pumping station downstream. Construction crews plan to remove about 6,500 cubic yards of gravel and rock to ease the problem. Bureau of Reclamation engineers are designing a jetty to redirect the river toward the pumping station. Construction likely will occur in midsummer when water flows are low. The bureau breached the dam to improve fish runs on the river.

Source: <http://www.kmed.com/pages/landing?2-9-10-GRAVEL-FROM-SAVAGE-RAPIDS-RECENTL=1&blockID=177632&feedID=133>

For more stories, see items [4](#) and [6](#)

[\[Return to top\]](#)

## **Public Health and Healthcare Sector**

34. *February 10, Los Angeles Times* – (California; National) **FDA addresses radiation safety.** The Food and Drug Administration (FDA) has decided to impose new safety controls on medical imaging devices and encourage development of more precise dosing standards in a bid to reduce unnecessary exposure of patients to diagnostic radiation. The agency also will promote a personal medical imaging history card that will enable patients to keep track of the number of images, and the amount of radiation, they receive over time, according to a medical imaging safety initiative unveiled Tuesday. The safety push comes months after Cedars-Sinai Medical Center in Los Angeles discovered that it had accidentally exposed more than 260 patients to eight times the normal dose of radiation for CT brain scans over a period of 18 months.

Source: <http://www.latimes.com/news/nation-and-world/la-na-fda10-2010feb10,0,115014.story>

35. *February 10, Gainesville Sun* – (Florida) **Stolen laptops place patients' data at risk.** The theft of two company laptops from AvMed Health Plans' corporate offices in Gainesville might have compromised the personal information of more than 200,000 current and former subscribers, as well as their dependents, the company has announced. The personal information includes names, addresses, phone numbers,

Social Security numbers and protected health information. The random way the data was listed, however, makes the risk of identity theft very low, the company said. The thefts were discovered on December 11. Potentially at risk are 80,000 current and 128,000 former subscribers dating back to April 2003, as well as their dependents.

Source: <http://www.heraldtribune.com/article/20100210/ARTICLE/2101062/-1/NEWSITEMAP>

For another story, see item [27](#)

[\[Return to top\]](#)

## **Government Facilities Sector**

36. *February 10, St. Tammany News* – (Louisiana) **Parish offices evacuated after suspicious box found.** Employees at the St. Tammany Parish Government offices at Koop Drive were evacuated for approximately two hours after someone noticed a very peculiar looking package. An official said the package was about the size of a cigar box, and it was covered in duct tape and was duct taped to the bridge that leads from the parish offices to the St. Tammany Tourist Commission offices. “It did look very suspicious,” she said, “because it was duct taped to the bridge. A spokesman for the St. Tammany Parish Sheriff’s Office said the department’s hazardous disposal unit was called out shortly after 11 a.m. and examined the box to make sure it did not contain anything dangerous. It was determined that the cardboard box was filled with paper and shortly after 1 p.m. employees were given the O.K. to return to their offices. The spokesman said it is unknown where the box came from or why it was on the bridge.

Source:

<http://www.slidellsentry.com/articles/2010/02/10/news/doc4b71ec9c705e5659459338.txt>

[\[Return to top\]](#)

## **Emergency Services Sector**

37. *February 9, North County Times* – (California) **Suspicious package found in fire station not dangerous.** The suspicious objects found in an Escondido fire station mailbox Tuesday morning were harmless containers, police said. The objects were found shortly after 9 a.m. by a postal carrier delivering mail to Fire Station No. 5 on Felicita Road and Monticello Drive, a fire captain said. Authorities temporarily shut down traffic in both directions on Felicita Road, an Escondido Police sergeant said, and the bomb squad was called to investigate. No other details were immediately available.

Source: [http://www.nctimes.com/news/local/escondido/article\\_97f02944-6a52-5c5c-8afa-38fcb9362fb5.html](http://www.nctimes.com/news/local/escondido/article_97f02944-6a52-5c5c-8afa-38fcb9362fb5.html)

38. *February 9, NBC Connecticut* – (Connecticut) **Blogger arrested over threat to cop: police.** Torrington, Connecticut police have a blogger accused of posting a threat

against a town police officer. On January 20, the Register Citizen newspaper in Torrington issued a complaint after learning that a threat was made on a newspaper blog against a Torrington Police officer, police said. The poster was anonymous and police investigated and determined that the threat came from a 26 year-old, of Stanfordsville, New York. He was arrested on Tuesday and charged with second-degree breach of peace.

Source: <http://www.nbcconnecticut.com/news/local-beat/Blogger-Arrested-Over-Threat-to-Cop-Police--83926312.html>

39. *February 9, Orange County Register* – (California) **Powder in sheriff's office is baking soda.** A Santa Ana, California, fire hazmat team was called to an Orange County Sheriff's administrative building Tuesday morning to investigate a white powder that was found in an envelope, authorities said. The white powder turned out to be baking soda, said a spokesman for the Orange County Sheriff's Department. The powder was in an envelope that was booked into evidence by La Habra police. The building was not evacuated.

Source: <http://www.ocregister.com/articles/powder-233316-white-sheriff.html?pic=1#article-read>

For another story, see item [47](#)

[\[Return to top\]](#)

## Information Technology

40. *February 10, The Register* – (International) **USB hack connects Droid to printers, video cams, and more.** A reverse engineering expert has disclosed a way to make his Motorola Droid host USB-enabled devices, a hack that allows the smartphone for the first time to directly connect to printers, video cameras, TV tuners, and a wide variety of other peripherals. The modification was devised by a researcher from Kismet and a researcher of OpenWRT and shared with the world by the chief hacker for reverse engineering firm H4RDW4RE. Using a charging cable that plugs into a car's cigarette lighter, a micro-USB cable, and a USB extender cable, he devised an improvised micro-dongle and connector cable. Getting the Droid to work with a Linux-enabled USB device is as simple as turning the smartphone off, connecting the cable to the host and peripheral and turning the Droid on. Once the Droid is booted, it should now work with the device. A user can even pull up a terminal and look at dmesg to see the usual kernel notifications that appear when new USB devices are connected. To be sure, the Droid is not the most robust of USB hosts. To change peripherals, a user needs to reboot the smartphone. What is more, leaving it plugged in too long causes the port to get stuck supplying power to devices but not actually recognizing them.

Source: [http://www.theregister.co.uk/2010/02/10/droid\\_usb\\_hack/](http://www.theregister.co.uk/2010/02/10/droid_usb_hack/)

41. *February 10, Webuser.co.uk* – (International) **2010 World Cup cybercrime site set up.** A new website is aiming to keep anyone looking for tickets or information about the 2010 World Cup safe from cybercriminals. The site, [www.2010netthreat.com](http://www.2010netthreat.com), has been set up by security firm Symantec to provide data, commentary, safety tips and

useful links for football fans following the 2010 World Cup tournament. There have already been a number of security threats relating to the 2010 World Cup spotted and Symantec has already warned that we should expect many more. A senior analyst at Symantec Hosted Services said: “Phishing attacks increased by 66 percent during the Beijing Olympics in 2008. The fact that two undersea communications cables landed on South African shores last July will exacerbate the threat levels; history also shows that malicious activity increases in a country after new bandwidth is made available,” he continued.

Source: <http://www.webuser.co.uk/news/top-stories/442112/2010-world-cup-cybercrime-site-set-up>

42. *February 9, Ars Technica* – (International) **Apple investigating Mac Pro performance and heat issues.** Recently, there have been some unusual issues affecting Nehalem-based Mac Pro models, characterized by abnormal performance degradation and CPU power draw when using on-board audio circuitry. Several sources have told Ars Technica that Apple support technicians are now saying the problem is known, and that the issue is being actively investigated by Apple engineers. The problem is most glaringly illustrated by merely playing music using iTunes. Though Activity Monitor will report just 1 to 3 percent CPU load, CPU power draw will increase tenfold and CPU temperatures will hover near the safe limits reported by Intel with little or no fan activity. Users were also able to reliably demonstrate a 20 percent decrease in performance, even with something as simple as plugging in FireWire or USB-based audio interfaces. Users note that the problem can be mitigated by using a PCIe-based audio card instead of on-board audio. So far, the problem has not been repeatable when the same Mac Pro hardware is booted into Windows, suggesting some conflict between Mac OS X and hardware drivers.

Source: <http://arstechnica.com/apple/news/2010/02/apple-investigating-mac-pro-performance-and-heat-issues.ars>

43. *February 9, Associated Press* – (International) **Summary Box: New attack shows security chip hole.** A former U.S. Army computer-security specialist has found a way to break into a type of chip that protects the most important secrets inside many personal computers. The specialist attacked a chip that carries a “Trusted Platform Module” designation, billed as among the industry’s most secure. The attack also works on other chips based on the same design and used in satellite television equipment, video game consoles, and smart phones. Smart and well-funded attackers could steal confidential documents from computers they have stolen, tap text messages and e-mail from lost or stolen mobile phones, and pirate satellite TV signals. The chip’s manufacturer knew this type of attack was possible, but determined it was so tough to pull off that it had limited chance of affecting many users.

Source:

<http://www.google.com/hostednews/ap/article/ALeqM5g8G9vF2KJnxKyTkqigqAyFda73HAD9DO7K103>

44. *February 9, Computerworld* – (International) **Researchers warn of likely attacks against Windows, PowerPoint.** Some of the bugs Microsoft patched on February 9

will be exploited by hackers almost immediately, security researchers predicted. Microsoft's massive update — a record-tying 13 separate security bulletins that patched 26 vulnerabilities — gives attackers all kinds of ways to compromise machines and hijack PCs. Even Microsoft said so: 12 of the 26 vulnerabilities, or 46 percent of the total, were tagged with a "1" in the company's exploitability index, meaning that Microsoft figures they will be exploited with reliable attack code in the next 30 days. But some of the flaws will be exploited long before others, said researchers interviewed on February 9. The manager of TippingPoint's Digital Vaccine group suggests that the vulnerabilities MS10-006 and MS10-012 could be exploited in a few days. MS10-006 and MS10-012 both involve SMB (Server Message Block), Windows file- and print-sharing protocols, but are not related.

Source:

[http://www.computerworld.com/s/article/9154438/Researchers\\_warn\\_of\\_likely\\_attacks\\_against\\_Windows\\_PowerPoint](http://www.computerworld.com/s/article/9154438/Researchers_warn_of_likely_attacks_against_Windows_PowerPoint)

45. *February 9, DarkReading* – (International) **China nudges out U.S. for most bot-infected machines.** The U.S. may still rank number 1 in spam production, but China is now home to the most bot-infected machines that spew spam, as well as the source of most SQL injection attacks. China made up 12.1 percent of all spamming bots or zombies as of last year's fourth quarter, while the U.S. dropped from 13.1 percent in the third quarter to 9.5, according to a new McAfee report. That puts the U.S. in the No. 2 position for bots. Interestingly, there has been a slow, downward trend worldwide in the number of newly infected bot machines spewing spam since June 2009, according to McAfee: That number went from 5 million in June and July to around 3.4 million in November, and then to about 3.9 million in December. Overall, spam volume has dropped during the winter months: After a record-breaking 175 billion spam messages per day in the third quarter, there was a 24 percent drop in the fourth quarter, to about 133 billion spam messages a day, McAfee says. McAfee says that trend will not last, however, because overall, spam volume is up 35 percent over the fourth quarter of 2008.

Source:

<http://www.darkreading.com/insidertthreat/security/client/showArticle.jhtml?articleID=222700604&subSection=End+user/client+security>

46. *February 9, The Register* – (International) **Feds say dev's 'cookie-stuffer' app fleeced eBay.** A Las Vegas web developer has been charged with fleecing eBay out of tens of thousands of dollars by selling a program that planted fraudulent web cookies on the PCs of people visiting the online auctioneer. Dubbed Saucekit, the program deposited a cookie on end users' hard drives that contained a unique code identifying affiliate websites even though advertisements from those sites were never viewed, according to documents filed on February 9 in U.S. District Court in San Jose, California. Users who went on to take "revenue actions" on eBay would cause the affiliate to receive a referral fee it was not entitled to. From January 2009 to the following November, Saucekit's creator actively promoted the cookie-stuffing program on his currently unavailable website and on hacking forums. Using the handle biglevel, he regularly discussed the technical and legal merits of the program. The

cookie-stuffing program exploited the eBay Partner Network, which pays referral fees to websites when one of their advertisements leads to a sale on the online auctioneer's site. The program works using web cookies that identify which site and advertisement were viewed just prior to the user visiting eBay. Saucekit directed user browsers to a website in Nevada, which deposited a cookie that identified a particular affiliate even though the website had not been visited.

Source: [http://www.theregister.co.uk/2010/02/09/ebay\\_cookie\\_stuffer\\_charges/](http://www.theregister.co.uk/2010/02/09/ebay_cookie_stuffer_charges/)

For another story, see item [17](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: <http://www.us-cert.gov>.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

## Communications Sector

47. *February 10, Ironton Tribune* – (Ohio) **Fire knocks out phone service.** Services on the Verizon phone lines in the Bradrick area of Chesapeake have been lost due to a structure fire. This will likely be an extended outage and affect a large part of eastern Lawrence County including parts or entire sections of Bradrick, Chesapeake, Union Township, Proctorville, Rome Township, and Athalia. The Lawrence County EMA office and 911 will be updated by Verizon as repairs progress. Early indications are that this will be an extended outage and that 911 calls will not be able to be made via land line from the affected area. The attached EAS message urges residents who need emergency assistance to use their cellular phones to report any law enforcement, EMS and fire. 911 centers in adjacent counties in Ohio, West Virginia, and Kentucky may experience additional calls from these affected areas. Procedures are in place in these counties to route calls to the Lawrence County 911 Center. The Lawrence County 911 Center is operating per normal procedures and will be working closely with these other counties to assure that emergency needs are taken care of as quickly as possible. Source: <http://www.irontontribune.com/news/2010/feb/10/fire-knocks-out-phone-service/>
48. *February 8, WWSB 7 Sarasota* – (Florida) **3 caught stealing copper from under Charlotte County bridge.** Charlotte County Sheriff's detectives arrested three people Saturday for cutting and stealing telephone copper wire under the U.S. 41 northbound bridge on the Port Charlotte side. A road deputy was flagged down about suspicious activity in that area and located three adults and two children. Deputies found holes exposing the phone cables which were cut with bolt cutters. A search of the vehicle located a shovel, posthole digger, and a bundle of copper wire. Two bolt cutters were found on the ground where the cables were cut. Detectives then charged all three adults with grand theft.

Source: <http://www.mysuncoast.com/Global/story.asp?S=11951454>

[\[Return to top\]](#)

## **Commercial Facilities Sector**

49. *February 10, Sayre Morning Times* – (Pennsylvania) **Chlorine leak leads to FD response. Lower level of Best Western sealed, evacuated after chlorine explosion.** A chlorine aerator exploded at the pool in the Best Western Grand Victorian Inn Tuesday afternoon, releasing a chlorine gas cloud that spread throughout the lower level of the hotel before it was contained by the Sayre fire department and later cleaned up by a Scranton-based hazardous materials team. The Sayre Fire Department was dispatched to the Fitness Express area in the basement of the hotel at 1:36 p.m. to respond to the incident, according to a report filed by a Sayre assistant chief. By the time firefighters arrived, staff had already evacuated the exercise rooms, and department members were able to enter using a self-contained breathing apparatus (SCBA) and remove the chlorine aerator from the building. Sayre firefighters were then able to seal off the fitness area and the rest of the hotel's lower level with duct tape and salvage covers. Best Western officials closed off the dining area, lounge and basement level to guests and staff during the response. One Best Western employee was transported to Robert Packer Hospital, where she was treated for chlorine gas intake and released. Additionally, an adult and child were treated at the scene by Greater Valley EMS personnel. Hotel guests were not evacuated at any point.  
Source: [http://www.morning-times.com/articles/2010/02/10/local\\_news/doc4b72b8db2c66c752506821.txt](http://www.morning-times.com/articles/2010/02/10/local_news/doc4b72b8db2c66c752506821.txt)

50. *February 10, WUSA 9 Washington* – (Maryland) **Large building collapsing under snow in Frederick.** Yet another building is in danger of collapsing under the weight of even more heavy snow in Maryland. A spokesperson for Frederick County fire and rescue says it is just a matter of time before a large metal frame building located on Monroe Avenue succumbs to the pressure of the heavy snowfall. He says crews were first alerted to the buckling building around 2:33 Wednesday morning. The roof of the building is sagging and dipping down between the support beams. The side of the building is also starting to cave in. He says approximately 21000 square feet of the 53000 square foot building is affected. The structure, owned by Ruppert Properties, houses a few businesses including the FCC Workforce Training Center.  
Source: <http://www.wusa9.com/news/local/story.aspx?storyid=96985&catid=158>

[\[Return to top\]](#)

## **National Monuments & Icons Sector**

51. *February 9, National Park Service* – (California) **Snow closes park facilities today.** The superintendent of Mammoth Cave National Park announced that most park facilities closed at 10:30 a.m. Tuesday because of conditions caused by a winter storm. Park maintenance crews and rangers will maintain the Mammoth Cave Parkway, the Park City Road, Cave City Road, Green River Ferry Road as long as conditions

remain safe. The Brownsville Road is closed, as well as Flint Ridge Road and Houchin Ferry Road. Green River Ferry will remain in operation as long as conditions remain safe. "Since last night we have had snow, then rain, then more snow," he added. "Temperatures are forecast to plummet this afternoon into the teens. We ask that all motorists obey road closure signs and drive slowly and carefully as they travel through the park."

Source: <http://www.nps.gov/mac/parknews/feb-9-snow-closures.htm>

[\[Return to top\]](#)

## **Dams Sector**

52. *February 10, Associated Press* – (Nebraska) **Corps says Neb. dams may have to be repaired.** Repairs may be required on five Lincoln and Omaha-area lake dams that the U.S. Army Corps of Engineers has determined may have potential seepage problems. The corps announced on Tuesday the potential problems exist along the outlet conduits at five Lincoln-area dams. They are located at Branched Oak, Holmes, Olive Creek, Wagon Train, and Stagecoach lakes. The corps is also reviewing whether the embankment of the dam at Glenn Cunningham Lake in Omaha is damaged. The potential problems were identified using a new dam-classification system used to screen dams. There is no evidence to suggest an emergency situation exists, or is about to occur, at any of the dams.

Source: <http://www.ktiv.com/Global/story.asp?S=11961991>

53. *February 8, New Orleans Times-Picayune* – (Louisiana) **Spillway Road closed because of high water.** Spillway Road in the Bonnet Carre Spillway is closed to traffic until further notice because of high water. The asphalt two-lane road between Norco and Montz in St. Charles Parish was closed Monday after the river level at the spillway rose to 13.31 feet at the Carrollton gauge in New Orleans, up .34 feet from Sunday. The river is expected to crest at 14.5 feet on Monday. Flood stage at New Orleans is 17 feet, and the area's levees are designed to handle levels of 20 feet. The Army Corps of Engineers has called a phase one "flood-fight" in which area levee district and corps employees inspect the levees twice a week.

Source:

[http://www.nola.com/traffic/index.ssf/2010/02/spillway\\_road\\_closed\\_because\\_of\\_high\\_water.html](http://www.nola.com/traffic/index.ssf/2010/02/spillway_road_closed_because_of_high_water.html)

For another story, see item [33](#)

[\[Return to top\]](#)

## **DHS Daily Open Source Infrastructure Report Contact Information**

**About the reports** – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **Contact Information**

Content and Suggestions:

Send mail to [NICCRports@dhs.gov](mailto:NICCRports@dhs.gov) or contact the DHS Daily Report Team at (202) 312-3421

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to [support@govdelivery.com](mailto:support@govdelivery.com).

---

### **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto:nicc@dhs.gov) or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.