Homeland Security

Daily Open Source Infrastructure Report for 14 February 2011

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- The Pittsburgh Post-Gazette reports an Indiana County, Pennsylvania, power plant already facing a series of pollution lawsuits was the scene of a steam pipe blast that injured six workers February 10. (See item **2**)
- According to the Associated Press, safety experts are puzzled about why reports of mistakes by U.S. air traffic controllers in the past year have nearly doubled in a time of unparalleled aviation safety. (See item **20**)

Fast Jump Menu

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 11, Associated Press* – (Ohio) **Massive gas explosion rocks Ohio countryside.** A gas pipeline explosion shook residents in Hanoverton, Ohio, February 10. The flames reportedly could be seen for miles around. A dispatcher for the Columbiana County Sheriff's Office said officials had no reports of injuries from the explosion and fire. She said there was no mandatory evacuation but those in the village of about 400 people and surrounding towns who wanted to leave their homes found

shelter at a school or at the Salineville Fire Department. The explosion occurred about 10:30 p.m. A television station initially reported one house caught fire, but a spokesman for El Paso Corp., which operates Tennessee Gas Pipeline, said there were no structural fires. One house was damaged, however, the company said. The explosion involved a 36-inch, buried transmission line that carries natural gas. Mechanisms in the section that "failed" automatically shut off the segment and the residual gas burned off, the spokesman said.
Source: http://www.msnbc.msn.com/id/41529771/ns/us_news-life/

2. *February 11, Pittsburgh Post-Gazette* – (Pennsylvania) **Six hurt in power plant blast.** An Indiana County, Pennsylvania, power plant already facing a series of pollution lawsuits was the scene of a steam pipe blast that injured six workers February 10. A 6-inch pipe containing steam under high pressure burst at 7:45 a.m. on the sixth floor of the plant's Unit One, said a spokesman for Edison Mission Group, the parent company of plant operator, EME Homer City Generating LP. The break in the pipe tripped the unit's automatic safety systems, shutting the unit down. The other two units were operating normally, he said. The rupture prompted an explosion of steam but did not cause a fire. The extent of damage has yet to be determined. Firefighters from the Coral/Graceton Volunteer Fire Department and the Homer City Fire Department were called to clear a landing site for three medical helicopters. Helicopters took three workers to West Penn Hospital, where a hospital spokeswoman said the men were in fair condition in the burn unit. The three other workers were driven to the Indiana Regional Medical Center, where they were treated and released, a hospital spokeswoman said. All of the employees at the 1,884-megawatt plant were evacuated and accounted for.
Source: http://www.post-gazette.com/pg/11042/1124627-455.stm

3. *February 11, Associated Press* – (Pennsylvania) **Search begins for clues in deadly Pa. explosion.** As the search for five victims of a massive explosion that rocked a Pennsylvania neighborhood reached its grim conclusion, the search for clues about what caused the disaster was in its beginning stages. The February 9 explosion in Allentown involved an underground gas main that lacked shut-off valves. It took utility workers 5 hours of punching through ice, asphalt, and concrete to seal the 12-inch main. The Lehigh County coroner said four bodies were recovered — a 4-month-old boy, a 16-year-old girl, a 69-year-old woman, and a 79-year-old man. Cadaver dogs found the fifth victim, a 74-year-old woman, in the rubble February 10. In all, 47 homes were damaged, and 8 appeared to be a total loss.
Source: http://www.google.com/hostednews/ap/article/ALeqM5hzrWXiAaO2dKZh-rptNi4RVfaKig?docId=e69970603cf14cdb996b218f0b3b78b0

4. *February 11, Cherry Hill Courier-Post* – (New Jersey) **Utility fined $200,000 for house explosion.** Public Service Electric & Gas (PSE&G) will pay a $200,000 fine for a house explosion that killed a 66-year-old Teaneck, New Jersey man. The state board of public utilities approved the settlement with the utility February 10. It also calls for PSE&G to revise procedures for reporting and tracking gas leaks. The utility agreed in November to pay $450,000 to the family of the victim. He died after leaking natural gas

ignited inside his home in July 2008.
Source:
http://www.courierpostonline.com/article/20110211/NEWS01/102110329/Utility-fined-200-000-for-house-explosion

[Return to top]

Chemical Industry Sector

5. *February 10, WDTN 2 Dayton* – (Ohio) **Hazmat cleanup needed at Calamityville.** It turns out a hazardous materials cleanup must happen before Calamityville opens in Fairborn, Ohio. The facility will help train emergency first responders in all manner of natural and man-made disasters. However, a chemical called TCE that is used in industrial cleaners was found on the site, and it exceeds the legal limit. According to the Xenia Gazette, a contract was awarded to A.S.T. Environmental, Inc. to begin cleaning Calamityville. The facility is expected to become fully operational in 2012.
Source: http://www.wdtn.com/dpp/news/local/greene_county/hazmat-cleanup-needed-at-calamityville

For another story, see item **31**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

6. *February 11, Associated Press* – (Vermont) **Vt business groups voice support for Yankee.** Vermont business and industry groups are renewing their call for the Vermont legislature and governor to support the continued operation of the Vermont Yankee nuclear plant. Associated Industries of Vermont, the International Brotherhood of Electrical Workers, and the Vermont Energy Partnership joined on February 10 urging the legislature to allow the public service board to rule on whether the plant should be granted a state certificate of public good to operate for 20 years past the expiration of its current license in March 2012. The groups said the nuclear plant in Vernon has been a reliable and affordable source of power in the state, important to industry and Vermont's overall economy. The governor reiterated his view that the plant is old and should be retired.
Source:
http://www.boston.com/news/local/massachusetts/articles/2011/02/11/vt_business_groups_voice_support_for_yankee/?rss_id=Boston.com+--+Local+news

[Return to top]

Critical Manufacturing Sector

7. *February 10, Recycling Today* – (New York) **OSHA proposes steep fine for New York foundry.** The U.S. Department of Labor's Occupational Safety and Health

Administration (OSHA) has cited Oberdorfer LLC for 28 alleged violations of workplace health and safety standards, including failing to correct hazards cited during a previous OSHA inspection. The Syracuse, New York, manufacturer of aluminum castings faces $220,000 in proposed fines following an OSHA inspection opened July 30, 2010, to verify correction of previously cited hazards. OSHA previously cited the company for a variety of violations involving employee overexposure to airborne concentrations of silica, which has been classified as a human lung carcinogen. This newest inspection found the company failed to implement engineering controls to reduce workers' exposure to silica. In addition, the inspection found that an employee who was overexposed to silica lacked a respirator.
Source: http://www.recyclingtoday.com/osha-proposes-fine.aspx

8. *February 10, Orange County Register* – (National) **UCI: 'Green' LED bulbs full of lead, arsenic.** The LED bulbs sold as safe and eco-friendly can contain high levels of lead, arsenic, and other hazardous substances, a new University of California, Irvine (UCI) study showed –- the same bulbs widely used in headlights, traffic lights, even holiday lights. The toxic material could increase the risk of cancer, kidney disease, and other illnesses, although the risks are more long-term than immediate; a single exposure to a broken bulb is unlikely to cause illness. "I wouldn't worry about an immediate release of vapor," said a UCI public health and social ecology professor, the principal investigator and an author of the study. "But still, when these residues hang around the house, if not cleaned up properly they could constitute an eventual danger." The lights should be treated as hazardous materials, and should not be disposed of in regular landfill trash, he said, because of the risk of the materials leaching into soil and groundwater.
Source: http://www.ocregister.com/news/bulbs-287781-ogunseitan-lights.html

9. *February 11, KCTV 5 Kansas City* – (Missouri) **Explosion injures worker at KC plant.** An explosion at an industrial plant in Kansas City, Missouri, burned one worker and caused damage to an exterior wall February 9. Around 10:30 a.m., fire crews responded to Kuhar Metallizing at 3825 Freemont St. One worker suffered minor burns and was taken to an area hospital as a precaution. Fire officials and company officials did not know what caused the explosion and are investigating.
Source: http://www.kctv5.com/news/26806201/detail.html

10. *February 11, Hazleton Standard Speaker* – (Pennsylvania) **Fire damages Weatherly foundry.** Firefighters from two counties battled a smoky blaze at Weatherly Casting & Machine Co. in Weatherly, Pennsylvania, for hours February 10. The company's president said the fire started around 12:30 p.m. in the oldest structure where the electric furnaces are located. The blaze sent smoke throughout the foundry, he said. Company officials accounted for all employees after they evacuated, and no one was injured, the president said. Employees were sent home, and the second shift of two was told not to report for work, he said. The president had no idea about the damage, and was waiting for firefighters to quell the flames, which went through the roof. He thought something either happened with the charge material or the furnace's new lining. The machine shop remained open as firefighters attacked the flames, which

could be seen at the apex of the roof which partially collapsed, according to reports. Firefighters from the Citizens Fire Co. No. 1 of Weatherly, L&L Fire Co., Tresckow Fire Co., Beaver Meadows Fire Co., and Freeland Fire Department responded. Weatherly Ambulance also responded.
Source: http://standardspeaker.com/news/fire-damages-weatherly-foundry-1.1103290

11. *February 11, WREX 13 Rockford* – (Illinois) **Back to normal after gas leak at Belvidere Chrysler plant.** Things are back to normal at the Chrysler plant in Belvidere, Illinois, after a gas leak February 10. A Chrysler spokeswoman said they found the leak just after 3 p.m. About 250 gallons of gas spilled out of a gasket on a pipe that carries fuel across the plant. The spokeswoman said employees were evacuated from that area and taken to a safe place away from the fumes. Second shift employees were sent home around 6:30 p.m. after a few dozen said they felt sick and had headaches. The spokeswoman said the Belvidere Fire Department came in to clean up and contain the leak and it gave the all clear shortly after 6 p.m. The gasket was replaced and third shift started on time at 11 p.m.
Source: http://www.wrex.com/Global/story.asp?S=14009774

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

12. *February 9, Softpedia* – (International) **RSA researchers confirm ZeuS code and features in SpyEye.** Security researchers from RSA have confirmed that the author of SpyEye is working on a "super trojan" by merging features from ZeuS into his own creation, sometimes by copying entire chunks of code. The most important addition from ZeuS so far is the HTML injection engine for Internet Explorer, which is a core component in such banking trojans. The author of SpyEye acknowledged that ZeuS's mechanism was practically copied it in its entirety without any major modifications. According to the RSA researchers, the main reason why ZeuS's injection component was better is its handling of cached pages. The old SpyEye mechanism was only capable of injecting code into HTML pages as they were being downloaded from the Internet, however, on repeated visits, the browser loads the page from its cache. Because of this, SpyEye deleted the cache after every injection to make sure the page is always downloaded from the server. Meanwhile, ZeuS is capable of injecting rogue code in cached pages, making its mechanism more reliable.
Source: http://news.softpedia.com/news/RSA-Researchers-Confirm-ZeuS-Code-and-Features-in-SpyEye-183464.shtml

13. *February 10, Help Net Security* – (International) **Credit score checking app triggers Trojan download.** The main reason people get scammed and/or their computer infected online is because they can not contain their curiosity, and that is precisely the thing on which the peddlers of a small application for checking credit scores and criminals records of Brazilian citizens count on. The application is offered for download on a public forum and is simple — it only presents the information harvested from public sites in a tidy manner: But unbeknownst to the user, the application also downloads a banking Trojan. That is why, Trend Micro researchers said, users should always keep in mind that a certain level of trust should be involved when it comes to installing and utilizing applications, and that they should download and install software only from verified sources.
Source: http://www.net-security.org/malware_news.php?id=1628

14. *February 11, Reuters* – (National) **Bank robbing 'Granddad bandit' pleads guilty.** A 53-year-old male, from Baton Rouge, Louisiana, pleaded guilty to 2 counts of bank robbery carrying a maximum penalty of 20 years in prison each as part of a plea agreement. In exchange, 24 other counts from robberies committed between 2008 to 2010 in 14 states outside of Virginia will not be charged against the suspect, according to a statement from the U.S. Attorney's Office for the Eastern District of Virginia. The robber admitted to robbing 26 banks throughout the country, including 2 in Virginia, by walking into each bank and passing a note to the teller that announced the robbery and stated the desired amount, the statement said. In court, the man said that he had stolen $83,868 in cash through his robberies.
Source: http://www.reuters.com/article/2011/02/11/us-robbery-granddad-idUSTRE71A3J120110211

15. *February 11, Houston Chronicle* – (Texas) **Hunt's on for Houston-area serial bank robber.** A man who held up a pair of banks in Spring, Texas, within about 30 minutes has been linked to at least four other similar robberies in the Houston area, FBI officials said February 10. The man struck about 1:30 p.m. February 9 at a Compass Bank branch in the 21000 block of Kuykendahl. About 2 p.m., the same robber demanded cash from employees at a Chase Bank branch in the 2100 block of FM 2920, officials said. The 2 banks are about 4 miles apart. No injuries were reported in either robbery, FBI officials said. The man is suspected in a recent string of area bank robberies beginning about 3 months ago. He is believed to have struck a Trustmark Bank branch November 16 in the 6800 block of FM 1960 West. On December 20, someone matching his description held up a Sterling Bank branch in the 800 block of FM 1960. He also hit a Regions Bank branch, 9480 College Park in The Woodlands, January 18 and February 1 robbed a Chase Bank branch in the 20700 block of FM 1485 in New Caney, FBI officials said. The robber is described as a 20- to 25-year-old clean shaven black man. He is about 5-feet-10 or slightly taller and has a slim build. The man wore a black knit cap, a dark sweater and pants, a white shirt with a dark tie and black-rimmed glasses, FBI officials said.
Source: http://www.chron.com/disp/story.mpl/metropolitan/7422432.html

[Return to top]

Transportation Sector

16. *February 9, United Press International* – (International) **Coyotes endangering airport's runways.** The airport at Canada's oil patch capital in Calgary, Alberta, is being plagued by roaming coyotes that threaten landing and take-off safety, regulators said. Since June, airport officials have filed 26 incident reports of the feral coyotes straying onto runways and prompting diversionary measures. This year alone, there have been four incidents, the Calgary Sun reported. A federal transportation safety board spokesman told the newspaper a 30-pound coyote was capable of doing "significant damage" to large aircraft. The airport's director of environmental service said attempts in Calgary and other airports to devise coyote-proof fences did not work, so his staff patrols the entire perimeter four times a day. He said a backhoe smashes coyote dens and holes under the fences are filled. However, the director said having some coyotes around is actually a benefit, as they help kill rabbits that attract large birds of prey, also a deadly danger to aircraft, the report said.
Source: http://www.upi.com/Top_News/World-News/2011/02/09/Coyotes-endangering-airports-runways/UPI-45721297255241/

17. *February 10, Reuters* – (International) **U.S. officials eye ways to increase airport security.** U.S. authorities are considering ways to tighten security in public areas at U.S. airports after a deadly attack in Moscow, Russia, last month, the head of the Transportation Security Administration (TSA), said February 10. A suicide bomber last month killed 36 people and injured more than 100 after detonating the device in the international arrivals hall of Moscow's busy Domodedovo airport, sending U.S. airport officials scrambling to address the security gap. The ideas included checkpoints before vehicles are allowed to pull up to the airport terminals, small security teams patrolling the grounds and using officers who are trained to detect unusual behavior, the TSA head told a House of Representatives' subcommittee on transportation security. U.S. authorities have ramped up security for air travelers, luggage and cargo in the wake of several attempts by al Qaeda militants to attack the United States, adding full-body scanners and requiring more screening for cargo.
Source: http://www.reuters.com/article/2011/02/10/us-usa-security-airports-idUSTRE7196WC20110210?feedType=RSS&feedName=domesticNews

18. *February 10, Scotsman* – (International) **Plane evacuation chaos at Glasgow Airport.** Passengers were injured in the evacuation of a plane at Glasgow Airport in Scotland, which was ordered by a cabin crew member without the knowledge of the pilots, according to the official investigation. There were reports of passengers from the Thomson Airways Boeing 757 coming down the emergency slides and colliding with those at the bottom, the Air Accidents Investigation Branch (AAIB) report said. Some passengers were concerned about the "apparent lack of assistance" once they had been evacuated after smoke was smelled on the plane, which had traveled from Madeira, Portugal with 238 people on board. The February 15, 2010 evacuation was ordered by the senior cabin crew member after normal disembarkation had started. Earlier, the flight crew had been aware of the smell and the co-pilot had briefly left the cockpit to investigate. Four passengers had minor injuries and "the flight crew were not aware an

evacuation had been initiated", the AAIB said.
Source: http://news.scotsman.com/news/Plane-evacuation-chaos-at-Glasgow.6715037.jp

19. *February 10, United Press International* – (National) **Napolitano: N.C. airport security failed.** U.S. airport security failed when a boy was able sneak onto a tarmac and stow away inside a passenger jet, the Homeland Security Secretary said. "Clearly if somebody — a 16-year-old — is able to circumvent [U.S. Transportation Security Administration (TSA)] standards and requirements and get into the wheel well of a plane, there has been a breakdown," she said at a congressional hearing February 9. The Secretary was referring to the boy, whose body was found in Milton, Massachusetts, November 15 after he sneaked onto North Carolina's Charlotte Douglas International Airport tarmac and climbed into the wheel well of a US Airways jet bound for Boston's Logan Airport.The National Counter-terrorism Center Director said he will work with the Homeland Security Secretary to determine if the United States had broader tarmac-security problems. TSA is investigating the incident. help / hide help
Source: http://www.istockanalyst.com/article/viewiStockNews/articleid/4881110

20. *February 11, Associated Press* – (National) **Air traffic control error numbers double.** Safety experts are puzzled about why reports of mistakes by air traffic controllers have nearly doubled in a time of unparalleled aviation safety in the United States. The Federal Aviation Administration said in the 12 months ending September 30, 2010, there were 1,889 operation errors — usually aircraft coming too close together. During the same period 1 year earlier, there were 947 errors. And the year before that — 1,008 errors. One air traffic controller at the facility in Ronkonkoma, New York, said there's a lax atmosphere in the control room. He said he's complained to the Transportation Department's Inspector General and to the Office of Special Counsel about controllers sometimes watching movies and playing with electronic devices during nighttime shifts when traffic is slower. The facility where the air traffic controller works handled the latest near midair collision of an American Airlines jet with 259 people aboard and two Air Force transport planes southeast of New York City.
Source: http://www.weartv.com/template/inews_wire/wires.national/2cde2cd8-weartv.com.shtml

For another story, see item **29**

[Return to top]

Postal and Shipping Sector

21. *February 10, Huntsville Times* – (Alabama) **Albertville woman charged with mailing 2 fake anthrax letters.** A federal grand jury has charged an Albertville, Alabama, woman with sending two fake anthrax letters to the local Social Security Administration (SSA) office. The 43 year-old woman faces two counts of mailing a

letter containing a powdery substance and a note to someone at the Albertville SSA. The powder did not test positive for any biological hazards. The U.S. Postal Inspection Service, the SSA Office of the Inspector General, and the Department of Homeland Security Federal Protective Service jointly investigated the case, which is being prosecuted by an assistant U.S. attorney.
Source: http://blog.al.com/breaking/2011/02/albertville_woman_charged_with_1.html

[Return to top]

Agriculture and Food Sector

22. *February 10, Wyoming Business Report* – (Wyoming; Montana) **Wyoming cow found with brucellosis.** The Wyoming Livestock Board announced February 9 it had received notice from animal health officials in Montana that a Wyoming cow at a Montana auction had serological evidence of brucellosis. The adult beef cow was from a ranch in Park County. State animal health officials are investigating the case, and making plans for further testing of the cow, as well as the herd she was from.
Source: http://www.wyomingbusinessreport.com/article.asp?id=56010

23. *February 10, Merced Sun-Star* – (California) **No injuries reported in Atwater Dole plant fire.** No one was hurt February 10 in a 1,000-square-foot fire at the Dole plant in Atwater, California, Merced County Fire Department officials reported. The cause is unknown, but it is believed to be accidental. The battalion chief said welding activities near the origin point may be responsible. Firefighters responded shortly before 4 a.m. and contained the fire within 90 minutes. The fire was extinguished by 6:30 a.m. Firefighters discovered the fire was about 30 feet from an ammonia tank. Firefighters were were able to keep the fire away from the tank. The fire burned a wall and entered an attic of the 50,000-square-foot building, which is partially enclosed. The damage was not severe enough to close the plant. The fire also burned part of the metal structure, construction insulation, and I-beams. The fire caused $30,000 to $35,000 in damage to the building, and $70,000 in damage to food-processing equipment. Seventeen firefighters, three Merced County Fire Department engines, an Atwater Fire Department engine, a Merced Fire Department engine, and a water tender responded.
Source: http://www.sacbee.com/2011/02/10/3392991/no-injuries-reported-in-dole-plant.html

24. *February 11, Food Safety News* – (National) **Smoked salmon recalled in 20 states for Listeria.** St. James Smokehouse Inc., of Miami, Florida, recalled 600 pounds of smoked salmon that was shipped to 20 states after routine sampling by the Florida Department of Agriculture and Consumers Services found the product may be contaminated with Listeria monocytogenes. The company recalled its Scotch Reserve Whiskey & Honey Smoked Scottish Salmon. The 4-ounce retail packs have the lot code 5797 and batch code 4759 with the UPC number 853729001151. No illnesses have been linked to the product. The recall was announced in a news release dated February 4 but published February10, by the U.S. Food and Drug Administration. The recalled salmon was distributed and sold at Fresh Market stores in Florida, North

Carolina, South Carolina, Tennessee, Georgia, Virginia, Kentucky, Alabama, Indiana, Illinois, Ohio, Louisiana, Maryland, Arkansas, Wisconsin, Mississippi, Pennsylvania, Massachusetts, Connecticut, and New York.
Source: http://www.foodsafetynews.com/2011/02/smoked-salmon-recalled-over-listeria-fears-1/

25. *February 11, Wisconsin Ag Connection* – (National; International) **Tyson pays $4 million to resolve foreign bribery allegations.** Tyson Foods Inc. has agreed to pay a $4 million criminal penalty to resolve an investigation into improper payments by company representatives to government-employed inspection veterinarians in Mexico, announced the assistant attorney general of the Criminal Division and the assistant director in charge of the FBI's Washington D.C. Field Office. "Tyson Foods used false books and sham jobs to hide bribe payments made to publicly-employed meat processing plant inspectors in Mexico," the assistant attorney said. A criminal information filed in U.S. District Court in the District of Columbia in connection with a deferred prosecution agreement charges Tyson with conspiracy to violate the Foreign Corrupt Practices Act (FCPA) and with violating the FCPA. Tyson, which is headquartered in Springdale, Arkansas, produces prepared food products. As part of a deferred prosecution agreement with the department, Tyson acknowledged responsibility for the actions of its subsidiaries, employees and agents who made improper payments to government-employed veterinarians who inspected two of its chicken processing plants in Gomez Palacio, Mexico. Court documents said the bribes were made to keep the veterinarians from disrupting the operations of the meat-production facilities.
Source: http://www.wisconsinagconnection.com/story-national.php?Id=304&yr=2011

26. *February 11, Food Safety News* – (International) **Toxic heavy metal found in Louisiana Gulf oysters.** Oysters collected from the Gulf of Mexico in Louisiana are turning up with extremely high levels of cadmium, a toxic heavy metal. The amounts — at 150 to 200 times greater than levels considered safe for human consumption — are troubling. Louisiana took the brunt of the 4.9 million barrel BP oil spill that flowed for 3 months in 2010. A marine biologist who works for the oyster industry from Mississippi sees two potential sources of cadmium. He said there is "anecdotal evidence" cadmium may be in the Louisiana Light Sweet Crude Oil that washed ashore from BP's free-flowing Macondo Well. "Therefore, oysters from areas that suffered direct oiling from the BP's spill may contain more cadmium than oysters from areas not receiving BP's oil," he said. The other potential source of the heavy metal would be the oysters themselves. He said oysters seem to be natural bioaccumulators of cadmium from seawater; there have been reports of concentrated cadmium in their shells at 1,000 times the background level. The latest oyster findings continue a trend in which local nonprofits and university researchers have come up with more unsettling findings than federal agencies, which have cleared Gulf seafood for human consumption almost from the day the oil stopped flowing.
Source: http://www.foodsafetynews.com/2011/02/toxic-heavy-metal-found-in-louisiana-gulf-oysters/

[Return to top]

Water Sector

27. *February 9, BrownwoodNews* – (Texas) **Cold weather slows down water treatment plant.** Officials at the Brown County Water Improvement District (BCWID) in Texas reported the recent cold snap has not only increased demand for water in the area, but also has slowed down the production capacity of one of the water treatment plants. The BCWID general manager said water temperature in the older west plant hit an all time low of 42 degrees Fahrenheit. "That cold of water is very difficult to treat," he said. "They [workers at the plant] have had some major problems treating that water, and they have had major problems with meeting the demand of our customers." He said the new microfiltration plant is better at filtering water at cold temperatures, but it is still only running at partial capacity due to equipment problems. The new plant is currently being used only as a backup to the older plant. The west plant should be able to put 10 million gallons per day through it he said, but at the colder temperatures, the plant can only treat between 4 to 6 million gallons through it per day. He said recently about 7 million gallons per day went through the microfiltration plant and another 4 million through the west plant treating 11 million gallons per day. He said this is more water running through the plants now than on some summer days. The increase in demand is due partially to a large amount of water leaks being reported in the area because of the recent cold weather.
Source: http://www.brownwoodnews.com/index.php?option=com_content&view=article&id=4378:cold-weather-slows-down-water-treatment-plant&catid=35:news&Itemid=58

28. *February 9, Associated Press* – (National) **EPA outlines how it will study fracking.** Even though there is mounting public pressure on the natural gas industry to rein in potential dangers associated with hydraulic fracturing, the practice is largely exempt from federal environmental regulation. The U.S. Environmental Protection Agency (EPA) has never investigated the process industry engineers use to extract gas trapped underneath shale deposits deep below the earth's surface — even though environmentalists allege fracking pollutes supplies of drinking water throughout the nation. A recent congressional inquiry found natural gas drillers had dumped more than 32 millions of diesel — one of several potentially hazardous byproducts of the fracking process — into the ground over a 5-year period. But now EPA is preparing a review aimed at possibly extending its oversight of fracking — and it has released an outline of how it will carry out its investigation. Under the preliminary version of the overhaul, EPA will investigate water contamination at three to five sites, as a sample from the far wider number of troubled fracking sites across the country. EPA investigators would also conduct two or three full case studies to examine the environmental effects of fracking over the full course of a cycle of gas extraction.
Source: http://news.yahoo.com/s/yblog_thelookout/20110209/ts_yblog_thelookout/epa-outlines-how-it-will-study-fracking

29. *February 10, KMOV 4 St. Louis* – (Missouri) **Multiple water main breaks causing problems in St. Louis.** In Missouri, the St. Louis City Water Division has its hands full dealing with several water main breaks across the city. The first in this string of water main breaks happened in January at Mississippi and Geyer. All lanes are still blocked in that area and are not scheduled to reopen until mid-February. A second water main break happened February 9 in north St. Louis. The break has not been fully repaired and all lanes of northbound Riverview between Hall and Scranton are still closed. The third happened February 10 on Sublette Avenue and Elizabeth Avenue in south St. Louis. The water division said this break will cause two problems. One is area residents will temporarily be without water. The other is that once the water is shut off, it will freeze on the streets, creating icy conditions. A fourth water main break happened February 10 on Hampton at Gresham. Water blocked one lane in that area.
Source: http://www.kmov.com/news/local/Multiple-water-main-breaks-causing-problems-in-St-Louis-115715639.html

30. *February 10, Courthouse News Service* – (Utah) **State tells Utah to clean it up.** A small central Utah water supplier's failure to monitor for feces should cost it big, no matter how many people drink from its well, the federal government said. Bristlecone Water Improvement District, near Bryce Canyon and Canyonlands National Parks, first failed to monitor for coliform and nitrate in 1999, and though the U.S. Environmental Protection Agency (EPA) asked Utah to take action in 2004, the state did not. Bristlecone's well serves about 160 people, including three residential hookups to seven full-time residents and seven outlets at two hotels, two restaurants, a RV park and a store, according to the federal complaint. The supplier failed to test its water annually through 2009, in violation of National Primary Drinking Water Regulations, federal prosecutors said. The EPA fined Bristlecone in 2004, but the company never paid up. All "'public water systems,' which provide water through pipes or other constructed conveyances to either 15 service connections or to 25 individuals at least 60 days per year" must monitor for bacteria, the complaint said. The federal government demands more than $6,000 in fines and civil penalties of up to $32,500 per day because Bristlecone's system tested positive for coliform in 2008.
Source: http://www.courthousenews.com/2011/02/10/34058.htm

31. *February 11, WPRI 12 Providence* – (Rhode Island) **Crews called to Portsmouth HAZMAT.** Crews were out for many hours February 11 dealing with a HAZMAT situation in Portsmouth, Rhode Island. The call came in shortly after 12 a.m. from the Newport Water Treatment Plant on West Main Rd. for reports of a chlorine leak. HAZMAT teams from East Providence and Newport Naval Base also reported to the scene. When crews arrived, they detected chlorine fumes inside the building, and said the cause was from a leaking valve assembly on a 1-ton tank. Three workers were inside the plant at the time of the incident, but no one was injured. By 6 a.m. HAZMAT teams had the situation under control. The wind was not a factor, so no nearby neighborhoods were evacuated.
Source: http://www.wpri.com/dpp/news/local_news/east_bay/crews-respond-to-hazmat-situation-at-newport-water-plant

[Return to top]

Public Health and Healthcare Sector

32. *February 10, Associated Press* – (Maine) **Salmonella outbreak reported at Maine facility.** Maine health officials said one person died February 2 after a salmonella outbreak at a retirement and assisted-living facility in Camden, Maine. The acting director of the Maine Center for Disease Control and Prevention, said seven cases of salmonella have been identified among residents at the Quarry Hill extended-care community. A spokesman for Pen Bay Health Care, the parent organization of Quarry Hill, told the Bangor Daily News the outbreak was noticed January 24 when several residents became ill with symptoms including diarrhea, cramps, headache, fever, and vomiting. One person was hospitalized and another person died February 2. Officials have not been able to trace the cause of the outbreak.
Source: http://www.necn.com/02/10/11/Salmonella-outbreak-reported-at-Maine-fa/landing_health.html?&blockID=3&apID=4cde8c64d5714b948243bdf14d67bd29

33. *February 11, WNYW 5 New York* – (New Jersey) **34 hospital patients exposed to TB.** Thirty-four employees at HealthSouth Rehabilitation Hospital in Toms River, New Jersey, have tested positive for exposure to tuberculosis (TB), hospital officials said February 11. They said no one has contracted the airborne disease that usually attacks the lungs. The hospital's CEO said the Ocean County Health Department and state health department have reviewed a list of every patient admitted during the past year. None were identified as known TB patients. She said exposure could have come from anyone. The CEO said there are no active TB cases and no risk to patients or workers. HealthSouth is a 98-bed acute rehabilitation hospital which opened in 1993 and has 400 employees.
Source: http://www.myfoxny.com/dpp/news/local_news/new_jersey/34-hospital-patients-exposed-to-tb-20110211-apx

34. *February 11, Homeland Security News Wire* – (National) **Tool developed to monitor pandemic threats.** Created with a grant from the U.S. Agency for International Development (USAID), an Emerging Pandemic Threats (EPT) tool, known as "Predict," will enable scientists and the public to track outbreaks of communicable animal diseases. The goal of the program is to preempt or combat, at their source, newly emerging diseases of animal origin that could threaten human health. The tool is being produced by experts on human and animal diseases from a consortium that first came together in 2009 during the pandemic of H1N1 swine flu. The experts have focused their attention on animal diseases that infect humans, such as the virus that caused the outbreak of SARS and the viruses (Ebola included) that are believed to have originated in bats. Predict will monitor data from 50,000 Web sites with information from World Health Organization alerts, online discussions by experts, wildlife trade reports, and local news. The EPT program is being managed by USAID with technical support from the U.S. Centers for Disease Control and Prevention and the U.S. Department of Agriculture.

Source: http://homelandsecuritynewswire.com/tool-developed-monitor-pandemic-threats

35. *February 11, Westmoreland Times* – (National) **Charges filed in health care fraud scheme.** An indictment was unsealed charging one man with health care fraud, and two other people with false statements relating to health care matters, according to U.S. federal officials. The defendants were arrested February 10. According to the indictment, the charges arose out of the defendants' operation of Advantage Ambulance Company, and a scheme to fraudulently bill Medicare by transporting patients by ambulance who were able to walk or travel by paratransit van.
Source: http://westmorelandtimes.com/news/2011/02/charges-filed-in-health-care-fraud-scheme-110211045301/

36. *February 11, New York Post* – (New York) **Municipal hospital system admits records were stolen.** The municipal hospital system disclosed February 11 confidential medical, personnel, vendor, and contractor records dating back 20 years at four Bronx, New York facilities were swiped in 2010 when a van was left unlocked and unattended. The Health and Hospitals Corporation (HHC) said it has begun notifying 1.7 million people affected by the theft involving Jacobi Medical Center, North Central Bronx Hospital, and 2 affiliated health centers. Officials said the stolen data was in the form of electronic files, but was "not readily accessible without highly specialized technical expertise and data-mining tools." They stressed there is no evidence any of the lost data has been accessed or misused. HHC offered 1 year of free fraud alert services for patients and others whose personal information may be at risk and is opening special customer care services February 14 at both hospitals. HHC said the theft occurred December 23, when a vehicle operated by its records vendor, GRM Information Management Services, was left unattended and unlocked while its driver made other pickups. The driver has since been fired. HHC also said it has terminated its contract with GRM and has filed a lawsuit to cover costs associated with the theft.
Source:
http://www.nypost.com/p/news/local/bronx/municipal_hospital_system_admits_QURUCV1SYV7r7E8Sv7kzqO

[Return to top]

Government Facilities Sector

37. *February 6, Washington Post* – (National) **Cost to build digital archive could hit $1.4 billion, federal auditors say.** The cost of building a digital system to gather, preserve and give the public access to the records of the federal government has ballooned as high as $1.4 billion, and the project could go as much as 41 percent over budget, government auditors reported February 4. The Government Accountability Office (GAO) blames the cost overruns and schedule delays on weak oversight and planning by the National Archives, which awarded a $317 million contract to Lockheed Martin 6 years ago to create a modern archive for electronic records. The Archives' largest and most complex capital project ever has been plagued by problems, and it is still

struggling to conduct effective oversight, auditors said. The Archives "has not been positioned to identify potential cost and schedule problems early and thus has not been able to take timely actions to correct problems and avoid program schedule delays and cost increases," the GAO wrote in its report.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2011/02/06/AR2011020603944.html

38. *February 7, Gainesville Sun* – (Florida) **Trial begins of UF professor, wife accused of fraud.** Attorneys made opening statements February 7 in the U.S. District Court trial of a former University of Florida professor and his wife who are accused of profiting from fraudulently obtained government contracts. The former UF nuclear engineering professor and his wife face 62 counts of wire fraud, money laundering, and other charges. An assistant U.S. attorney said they obtained contracts from NASA and the Air Force under false pretenses for a decade. They made more than $1 million from the scheme, he said. The professor started at UF in 1980 and was director of its Innovative Nuclear Space Power and Propulsion Institute. He and his wife also operated a Gainesville-based research company, New Era Technology, that obtained nearly $3.4 million in government contracts since 1999, according to court documents.
Source: http://www.gainesville.com/article/20110207/ARTICLES/110209530/1109/sports?Title=Trial-begins-of-UF-professor-wife-accused-of-fraud&tc=ar

39. *February 8, Government Computer News* – (International) **White House attack e-mails were faked, says UK official.** A cyberattack targeting British officials, which at first appeared to be carried in White House e-mails, actually originated in China, with the perpetrator using a hoax e-mail address that resembled a White House account, officials in the United Kingdom said. Nevertheless, U.K. officials are using the opportunity to call for more cooperation among governments to jointly agree on policies for state-based covert cyber activity. The initial reports February 4 from the British foreign secretary indicated e-mail messages alleged to be from the White House were sent to several British officials in late December. The e-mails contained links that, if opened, would download a virus onto the user's computer. It was first unclear if the attack came from authentic White House e-mail accounts that had been hacked and infected with a virus or from fake e-mail accounts made to resemble White House e-mail messages. In recent days, the latter scenario appears the more likely. Although the foreign secretary did not name the country behind the attacks, intelligence sources familiar with the incidents made it clear the originating country was China, the Guardian said in an article February 4.
Source: http://gcn.com/articles/2011/02/07/alleged-white-house-email-cyberincident-now-called-spoof-attack-from-china.aspx

40. *February 11, KGTV 10 San Diego* – (California) **Brush fire quickly extinguished on Marine base.** A 2-acre fire that may have been sparked by a Marine Corps artillery shell was extinguished February 10 at Camp Pendleton in California, authorities said. The fire began around 9 p.m. and spread to San Clemente, a Los Angeles television station reported. The Marine Corps base fire department is investigating how the fire

started, authorities said.
Source: http://www.10news.com/news/26831158/detail.html

For more stories, see items **21** and **58**

[Return to top]

Emergency Services Sector

41. *February 7, Houston Chronicle* – (Texas) **Former Harris Co. sheriff's deputy pleads guilty in drug case.** A former Harris County, Texas sheriff's deputy suspected of using his badge and gun to stop drug dealers and steal their loads pleaded guilty February 7 to federal extortion charges. The 43-year-old, entered a guilty plea before a U.S. district judge, admitting his role in a drug deal that was actually an undercover sting set up in December 2010 by Houston police and FBI agents. He was arrested wearing his sheriff's uniform and carrying his gun. He and four Houston men were arrested together December 15 after the deputy followed an SUV driven by a Houston Police Department (HPD) officer posing as a Mexican drug courier. One of the men arrested entered the SUV and retrieved a package containing a 2-kilogram load of fake cocaine. The HPD undercover officer left the SUV and walked into a sporting goods store. The former deputy and two other men were stopped as they left with the contraband. The former deputy is free on bond. He faces up to 20 years in federal prison without parole and a $250,000 fine.
Source: http://www.chron.com/disp/story.mpl/metropolitan/7417241.html

42. *February 9, Arizona Republic* – (International) **U.S., Mexico police unite to fight border crime.** Top Homeland Security officials said February 8 that a little-known coalition of U.S. and Mexican police agencies has played a major part in cracking down on smuggling and illegal immigration along the Arizona-Mexico border. The joint operation between the U.S. Border Patrol, Mexican federal police, and about 60 U.S. state, federal, tribal, and local police agencies has had success in making drug seizures and arresting undocumented immigrants, the director of Customs and Border Protection said. Since the Alliance to Combat Transnational Threats launched in September 2009 with coordinated training, intelligence-sharing, and patrols, the program has resulted in the arrest of 270,000 illegal border crossers, the seizure of 1.6 million pounds of marijuana, and the recovery of $13 million in cash in the border's Tucson Sector. The alliance issues weekly intelligence briefings on security threats for all border agencies.
Source: http://www.azcentral.com/community/pinal/articles/2011/02/09/20110209us-mexico-fight-border-crime.html

43. *February 10, Associated Press* – (International) **Military radar sought for northern drug crackdown.** U.S. Senators from states along and near the nation's northern border requested February 10 that the Department of Defense provide military radar to crack down on drug trafficking by low-flying aircraft. Drug smuggling across the border with Canada is much more prevalent than indicated by the number of cases

where drugs have been seized, according to a federal report from November 2010 and recent media stories, a New York Senator said. Less than 1 percent of the 4,000 mile border is considered under the operational control of U.S. border officials, according to a General Accountability Office (GAO) report released in February. Most areas of the northern border are remote and inaccessible by traditional patrol methods. Customs and Border Protection believes it can detect illegal entries, respond, and deal with them on only about 32 miles of the northern border. The Border Patrol was aware of all illegal border crossings on only 25 percent of the border, or 1,000 out of 4,000 miles, the GAO report said.
Source: http://www.forbes.com/feeds/ap/2011/02/10/general-us-border-security-northern-border_8301578.html

44. *February 10, Global Security Newswire* – (National) **Justice department remains lacking on WMD response, official says.** The U.S. Justice Department's (DOJ) efforts to prepare for a potential weapons of mass destruction (WMD) attack have been "uncoordinated and fragmented," the acting Inspector General said February 9. She said while the FBI had made adequate preparations for dealing with the fallout of a WMD assault, other branches of DOJ and the organization in total had not put in place appropriate measures, the Washington Times reported. DOJ has not selected an office or individual as a core supervisor for WMD response operations, she said in testimony before a U.S. House of Representatives subcommittee. With the exception of the FBI, department subunits have supplied zero or nearly zero applicable training and generally avoid taking part in WMD drills.
Source: http://www.globalsecuritynewswire.org/gsn/nw_20110210_1106.php

45. *February 10, Federal Bureau of Investigation* – (California) **Seal Beach woman arrested for impersonating FBI agents.** A Seal Beach, California woman was arrested February 10 for allegedly used "spoofing" technology to impersonate FBI agents in phone calls to business clients who believed she was running a fraud scheme, announced the assistant director of the FBI in Los Angeles, California, and a U.S. attorney. The 44-year-old is charged with impersonating a federal agent in a criminal complaint filed February 8. According to the affidavit in support of the complaint, she operated a real estate service that charged clients a $30,000 "consulting fee" for providing unique information about favorable commercial properties. When some clients concluded she failed to deliver the promised services, they complained on an Internet blog and encouraged others to report her suspected fraudulent activity to the FBI and other federal authorities. Near the end of 2010, one of her unsatisfied clients was contacted by a caller with a male voice who claimed to be an FBI agent and whose caller ID was for the main number of the FBI's Los Angeles Field Division. In this call, the "agent" threatened to imprison the woman's client if she did not stop complaining about her. Subsequent investigation revealed calls from the purported male FBI agent were actually made from the woman's cellular phone, who used a Web site to alter her voice and to alter her caller ID to "spoof" the FBI's Los Angeles Field Division's phone number.
Source: http://losangeles.fbi.gov/pressrel/pressrel11/la021011.htm

46. *February 11, Associated Press* – (South Carolina) **Unmarked SC police cruiser stolen, found abandoned.** Berkeley County, South Carolina sheriff's deputies said an unmarked cruiser was stolen and later found abandoned in Goose Creek February 10. A sheriff's spokesman said there was at least one gun in the car that belonged to the deputy driving the vehicle. It was unclear if the gun was still in the car when it was found shortly after 11 p.m. The spokesman said the county jail director was apparently in a home in the Goose Creek area when the car was taken. No arrests have been reported.
Source: http://www.thesunnews.com/2011/02/11/1975743/unmarked-sc-police-cruiser-stolen.html

[Return to top]

Information Technology Sector

47. *February 9, Softpedia* – (International) **Security fixes available for Shockwave Player and ColdFusion.** Adobe has released security updates for its Shockwave Player and ColdFusion products to address critical vulnerabilities that could be exploited to compromise computers and information. The new Shockwave update fixes 21 security flaws that could lead to arbitrary code execution. The vulnerabilities are located in modules such as dirapi.dll, IML32, TextXtra, Shockwave 3D Asset, Font Xtra.x32, and other unspecified components. Adobe also released hotfixes for ColdFusion 9.0.1, 9.0, 8.0.1, and 8.0, which address five vulnerabilities on the platform. These security issues consist of two cross-site scripting weaknesses in the administrator console and the cfform tag, a CRLF injection flaw which allows adding headers, an information disclosure vulnerability, and a Session Fixation bug.
Source: http://news.softpedia.com/news/Security-Fixes-Available-for-Shockwave-Player-and-ColdFusion-183442.shtml

48. *February 9, Panda Security* – (International) **January malware update: PandaLabs found 43 percent of US PCs were infected.** PandaLabs, Panda Security's anti-malware laboratory, announced findings February 9 based on data from scans completed by Panda ActiveScan, the free online scanner offered by Panda Security, The Cloud Security Company. In January, PandaLabs found 43 percent of U.S. computers scanned were infected with malware, compared to 50 percent of total global users scanned. Trojans were found to be the most prolific malware threat, responsible for 58 percent of all U.S. cases, and 59 percent globally. The next most common culprits were traditional viruses and worms which caused 12 percent and 9 percent of cases worldwide, respectively. Although the United States made the top 10, Thailand, China, Taiwan, Russia, and Turkey held the top 5 highest rates of infection, ranging from 60 to 67 percent of cases. And with a 43 percent infection rate, the U.S. ranked tenth, only a few percentage points below historical "malware havens," such as Brazil and Poland. Of the most prevalent malware threats detected this January, generic Trojans topped the list, followed by downloaders, exploits, and adware. Panda found the "Lineage" Trojan continues to spread and infect systems, indicating a lack of basic antivirus protection for even the most longstanding threats.

Source: http://www.prnewswire.com/news-releases/january-malware-update-pandalabs-found-43-percent-of-us-pcs-were-infected-ranking-tenth-worldwide-115632469.html

49. *February 10, Computerworld* – (International) **Low security awareness found across IT.** A broad spectrum of IT people, including those close to security functions, appear to have little awareness of key security issues impacting their organizations, a new survey showed. The survey, which polled 430 members of the Oracle Application Users Group conducted by Unisphere Research and sponsored by Application Security Inc. included directors and managers of information technology, developers and programmers, database and systems administrators, systems architects and analysts, and professionals from the HR and financial functions. About 22 percent of respondents claimed to be extensively involved in security functions, 60 percent claimed a limited or supporting role, and the rest said they were not involved with security at all. About 100 respondents belonged to companies with more than 10,000 employees. What the survey showed was a surprising lack of awareness of security issues among the respondents. For instance, just 4 percent admitted to being fully informed about security breaches within their organizations. About 80 percent of those who said their organizations had suffered a data breach in the past year were unable to tell which IT components might have been impacted by the breach.
Source:
http://www.computerworld.com/s/article/9208890/Low_security_awareness_found_across_IT_

50. *February 10, Computerworld* – (International) **Vendors tap into cloud security concerns with new encryption tools.** A handful of vendors have begun rolling out technologies designed to let companies take advantage of cloud computing environments without exposing sensitive data. One vendor, CipherCloud, a Cupertino, California-based start-up, launched a virtual appliance technology February 10 that companies can use from within their premises to encrypt or to mask sensitive data before it hits the cloud platform. Unlike the case with encryption services offered by cloud providers, CipherCloud's technology lets enterprises have complete control over the encryption and decryption process, the CEO and founder of the company said. The only set of encryption keys resides with the enterprise and not the cloud provider, ensuring that only authorized users can view the data, he said. CipherCloud's algorithm works in a way that encrypts data without fundamentally altering the data format or function, he added.
Source:
http://www.computerworld.com/s/article/9208882/Vendors_tap_into_cloud_security_concerns_with_new_encryption_tools

51. *February 10, Help Net Security* – (International) **Multiple vulnerabilities in Django.** Vulnerabilities have been reported in Django, which can be exploited by malicious people to bypass certain security restrictions and conduct script insertion and cross-site request forgery attacks, Secunia said. The first vunerability is the cross-site request forgery protection does not properly verify requests with certain "X-Requested-

With" headers that can be exploited to conduct attacks by using certain browser plugins and HTTP redirects to send cross-domain HTTP requests with spoofed headers. The second vulnerability is input passed via the filename of uploaded files is not properly sanitized within the file field before being used. This can be exploited to insert HTML and script code that will be executed in a browser session in context of an affected site if malicious data is viewed. Successful exploitation requires a file-storage backend that does not properly sanitize the file name used (no default file-storage backends are affected). Lastly, the file-based session storage system does not properly sanitize the key submitted in the session cookie, which can be exploited to conduct directory traversal attacks.
Source: http://www.net-security.org/secworld.php?id=10571

52. *February 11, Help Net Security* – (International) **Organizations spend 127 hours per month managing on-site security solutions.** Organizations spend an average of 127 hours per month managing on-site security solutions and related problems, according to new research from Webroot. The top time thieves are updating software and hardware, re-imaging infected machines, and enforcing end user Internet and e-mail policies. Webroot surveyed 820 IT decision-makers in organizations with 100 to 5,000 employees in the United States, the United Kingdom, and Australia. The company found organizations with more remote or mobile employees face more problems when using on-premise security. Specifically, these companies are 43 percent more likely to experience phishing attacks and 33 percent more likely to experience viruses or worms than organizations using cloud security. Time spent repairing damage and addressing other repercussions is also more significant.
Source: http://www.net-security.org/secworld.php?id=10575

53. *February 11, The Register* – (International) **Malware endemic even on protected PCs.** Many users remain infected with computer malware despite the fact the vast majority are running machines protected by anti-virus software, according to a study by European Union statistics agency EUROSTAT. The study found one-third of PC users (31 percent) were infected even though the vast majority (84 percent) were running security software (anti-virus, anti-spam, firewall) on their PCs. Of the survey's respondents, 3 percent reported financial loss as a result of farming or phishing attacks, while a further 4 percent reported privacy violations involving data sent online. Bulgaria (58 percent) and Malta (50 percent) top the list of most infected users. By comparison, Finland (20 percent), Ireland (15 percent), and Austria (14 percent) did relatively well. Trojans (59.2 percent) were the most common types of infected found on compromised PCs, followed by viruses (11.7 percent).
Source: http://www.theregister.co.uk/2011/02/11/malware_endemic_survey/

For another story, see item **12**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: http://www.us-cert.gov

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

[Return to top]

Communications Sector

54. *February 10, TMCnet* – (International) **Egypt shut down most of internet service by pulling single switch in Cairo.** It is being reported that when Egyptian officials wanted to shut down Internet service last month — they did it the easy way: They pulled a single switch. Wired.com said recently the Egyptian government shut down most of the Internet service by pulling a switch in a data center located in Cairo. It had been speculated Egyptian officials had called Internet Service Providers (ISPs), one after another. Word of their approach comes from information presented by the U.S. Department of Homeland Security's Infosec Technology Transition Council. "Most of the outage was effected through a breaker tripped in the Ramses exchange, and the rest was phone calls and arm-twisting," Wired.com said, citing information from the presentation. Ramses exchange is located in a building in Cairo, "where Egyptian ISPs meet to trade traffic and connect outside of the country," according to Wired.com. It is referred to as an Internet Exchange Point. Wired.com said turning off the Internet there made it easier to turn it back on, was more secure, and kept "spyware from being placed on the networks." Given the millions of dollars it cost the economy, while the Internet was turned off, the presentation concluded it will be "unlikely that Egypt's communications ministry will ever be asked to flip that switch again." Forbes magazine estimated it cost the Egyptian economy $110 million. The Egyptian vice president estimated that the impact on the tourism sector was "at least $1B (billion)."
Source: http://ipcommunications.tmcnet.com/topics/ip-communications/articles/143626-egypt-shut-down-most-internet-service-pulling-single.htm

[Return to top]

Commercial Facilities Sector

55. *February 11, Petersburg Progress-Index* – (Virginia) **Meth lab found in Chesterfield hotel room.** Virginia State Police arrested a Florida man and charged him with manufacturing drugs after a traffic stop for expired license plates and a search of his Chesterfield hotel room led to the discovery of a methamphetamine lab February 9. Shortly before 9 a.m. a citizen told a trooper about suspicious activity in the area and provided information on the suspect to the officer. The trooper then saw the suspect getting into a vehicle and initiated a traffic stop based on expired license plates.

According to a state police sergeant, based on information received from the suspect and after an affidavit for a search warrant was obtained, a search of the suspect's room was conducted. Six other rooms were evacuated as a precautionary measure. Inside the hotel room, authorities found an active meth lab. Officials said that the suspect had been in the room for several days. The suspect has been charged with one count of manufacturing a controlled substance (methamphetamines), which is a felony.
Source: http://progress-index.com/news/meth-lab-found-in-chesterfield-hotel-room-1.1103418#axzz1Df5C3z00

56. *February 11, Berkshire Eagle* – (Massachusetts) **Roof collapses on Hubbard Ave. commercial building.** Heavy snow triggered a commercial building's roof collapse that nearly blew the structure apart sometime February 9 or February 10 in Pittsfield, Massachusetts. The building has been declared a total loss. The collapse at 446 Hubbard Ave. involved a commercial structure owned by Allegrone Construction Co. of Pittsfield and rented by Collins Electric and The Overhead Door Co. of Pittsfield. The 6,000-square-foot building had a pitched roof, but the snow and ice buildup was too much for the wooden trusses to handle, according to a city building commissioner. "When the roof collapsed, it blew out the garage bay doors rated to withstand a 100 mph wind," he said. "Even one wall was starting to lean. It's a total loss." He was unable to give an estimated cost of damage to the building and its contents.
Source: http://www.berkshireeagle.com/local/ci_17351269

[Return to top]

National Monuments and Icons Sector

57. *February 10, Associated Press* – (Virginia) **Potentially live Civil War-era shell discovered by National Park Rangers at Virginia home.** National Park Rangers said they found a potentially live Civil War-era artillery shell February 10 in Petersburg, Virginia, and have called in police to check it out. The shell was found at a home after rangers with a warrant searched it during a criminal investigation. The Petersburg Progress-Index newspaper reported local police blocked off streets near the home while state police retrieved the shell. Officials could not say whether the shell was live. Civil War-vintage shells are often recovered in Virginia.
Source:
http://www.google.com/hostednews/canadianpress/article/ALeqM5jYVZffhMZgGWXn3iVbcjEN3ffEKQ?docId=5915251

[Return to top]

Dams Sector

58. *February 11, Associated Press* – (National) **Fargo school raising floodwall, cofferdam.** A Fargo, North Dakota, school that was heavily damaged by Red River floodwaters in 2009 is taking more precautions as this year's spring flooding season nears. Oak Grove Lutheran School is adding 2 feet to the permanent floodwall on the

school's east side to protect to a river level of 42 feet. The school also plans to raise the top of its steel cofferdam by 1 foot, using plywood and plastic. Floodwaters forced their way under the dam 2 years ago, inundating 2 buildings and causing $1.8 million in damage.
Source: http://www.thedickinsonpress.com/event/apArticle/id/D9LAL4GO0/

[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 Web site: http://www.dhs.gov/iaipdailyreport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
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.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at 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 or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer