Daily Open Source Infrastructure Report
2 February 2012

Top Stories

- Four men inspired by al-Qa'ida admitted planning to detonate a bomb at the London Stock Exchange, and considered targeting the U.S. Embassy. – *BBC News* (See item **14**)
- Police found several bombs and ingredients to make more explosives inside an apartment in Fort Wayne, Indiana, while the man who lived there remained hospitalized after his hand was blown off in an explosion January 29. – *Fort Wayne Journal Gazette* (See item **56**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *February 1, Houston Chronicle* – (Texas) **Houston misses EPA deadline to correct air pollution — by 28 years.** The Environmental Protection Agency (EPA) concluded January 31 that Houston, has failed to meet 30-year-old limits on smog-forming pollution, a decision that could lead to hefty fines for as many as 300 oil refineries, chemical plants, and other large industrial facilities. The EPA made the determination 6

months after a settlement with the Sierra Club, which had accused the federal government of skirting its obligation to enforce the rules set in 1979. Houston had a 2007 deadline to comply with the smog limits but fell short despite significant improvements in air quality. Federal law requires the state to collect fines from the eight-county region's largest polluters until the standard is met. It is unclear how the Texas Commission on Environmental Quality would implement the penalty program. The state agency was about to finalize procedures, but shelved them on the EPA's advice last year. The EPA had said Houston and other places still in violation of a smog standard set 3 decades ago would not have to pay fines if they met a newer, more stringent limit for the widespread air pollutant. The federal guidance was vacated last year by the U.S. Court of Appeals for the District of Columbia Circuit.
Source: http://www.dailycomet.com/article/20120201/WIRE/120209997?tc=ar

2. *January 31, Amarillo Globe-News* – (Texas) **Copper spools worth $10K stolen from Xcel.** Amarillo, Texas police are seeking four large spools of copper wire taken from an Xcel Energy site, the Amarillo Globe News reported January 31. On January 24, Xcel Energy reported four commercial-grade copper spools worth more than $10,000 missing from its property. Police said property surveillance equipment recorded a four-door Nissan Frontier hauling a red trailer in the area. An Xcel Protection Services consultant said the 3- and 4-foot copper spools were going to be used for new construction. Three of the spools were small enough to load onto the truck or trailer and the fourth was likely rolled on. The stolen copper was insulated, or covered with plastic, which is typically harder to recycle.
Source: http://amarillo.com/news/local-news/2012-01-31/more-10k-copper-stolen-xcel-site#.TylMnoHLlBk

3. *January 28, Bay City News* – (California) **CPUC fines PG&E $16.7 million.** The California Public Utilities Commission (CPUC) fined Pacific Gas & Electric (PG&E) more than $16 million January 27 for failing to conduct gas pipeline leak surveys on a stretch of pipeline in Contra Costa County. PG&E said it was "surprised" by the $16.7 million fine, since the utility self-reported the problem to the state regulatory agency in December, and has taken steps to survey the 14 miles of affected pipeline and repair the 22 leaks subsequently discovered. PG&E apparently failed to conduct regular surveys of the pipelines because the utility's maps were not updated to accurately reflect new construction. While some of the construction occurred within the past 5 years, in other places the violations date back to 1993, according to the citation. The penalty is the first under a new program authorizing CPUC staff to issue fines without the approval of the commission. Approved in December, the program is one of many changes the agency made in response to the September 2010 San Bruno pipeline explosion, which killed eight people, injured scores of others, and destroyed dozens of homes.
Source: http://abclocal.go.com/kfsn/story?section=news/local/east_bay&id=8522429

[Return to top]

Chemical Industry Sector

4. *February 1, Reuters* – (California; International) **U.S. accuses China of instigating plot against DuPont.** Chinese government representatives directed a U.S. businessman to obtain valuable technology manufactured by chemical giant DuPont, according to newly released court documents. They said U.S. authorities were seeking February 1 to keep the man in jail ahead of his trial on charges relating to trade secret theft. The businessman, and his wife, each were indicted last year by a Northern California grand jury on three counts, including witness tampering, making a false statement, and conspiracy to tamper with witnesses and evidence, the court documents said. A bail hearing was scheduled for February 1. According to court documents, the man paid at least two former DuPont engineers for help in designing chloride-route titanium dioxide. DuPont is the world's largest producer of the white pigment used to make a range of white-tinted products, including paper, paint, and plastics. The man and his wife have pleaded not guilty. The man was held without bail, while his wife was released, court documents show.
   Source: http://www.reuters.com/article/2012/02/01/us-china-usa-dupont-idUSTRE8100OP20120201

5. *February 1, Alexandria Daily Town Talk* – (Louisiana) **2 truckers die in collision on La. 28 in Vernon Parish.** A collision of two 18-wheelers — including one carrying molten sulfur — early January 31 killed both drivers and blocked the intersection of La. Highways 28 and 8 east in Vernon Parish, Louisiana, for about 11 hours. The crash occurred about 4:10 a.m. when one truck ran a stop sign and collided with the other truck. The wreck closed the highways to traffic, and haz-mat units from the Louisiana State Police and Fort Polk responded. One truck was carrying molten sulfur, while the other was a log truck. The sulfur didn't spill on the roadway, and the highways reopened around 3 p.m.
   Source: http://www.thetowntalk.com/article/20120201/NEWS01/202010325/2-truckers-die-collision-La-28-Vernon-Parish

For more stories, see items **1**, **32**, and **38**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

6. *February 1, Pennsylvania Department of Environmental Protection* – (Pennsylvania) **Pennsylvania DEP seeks information about antique medical kit containing radium-226.** The Pennsylvania Department of Environmental Protection (DEP) announced February 1 it is asking anyone who knows the history of an antique medical kit containing about one curie of radium-226 found in a Chester County trash bin to contact the agency's bureau of radiation protection. The material was found January 19, when a load of construction debris set off radiation alarms at Waste Management Inc.'s Norristown transfer station. The company deployed a health physicist to recover the material. Exposure to one curie of radium-226 is equivalent to having more than 100

CT scans at once, and it has the potential to create skin burns within a few hours of contact. DEP health physicists traced the kit's source to a roll-off container that had come from the Hershey's Mill retirement community in West Chester. "Although the capsules do not appear to be leaking, we believe that someone could have had direct contact with these sources of radium-226," the bureau director said. "The radioactive radium they contain is about five times the amount found in modern medical sources, and we are concerned about the health of anyone who may have handled them." Source: http://www.marketwatch.com/story/pennsylvania-dep-seeks-information-about-antique-medical-kit-containing-radium-226-2012-02-01

7. *January 31, Associated Press* – (Illinois) **NRC inspecting water pumps at stalled US reactor.** A failed electrical insulator blamed for a power loss to a nuclear reactor near Byron, Illinois, was replaced January 31, and the Nuclear Regulatory Commission (NRC) began a special inspection into how reactor water pumps responded to the outage, officials said. Exelon Energy began preparations to re-start the Unit 2 reactor at the Byron Generating Station, though it was unclear how soon it could return to service, a spokesman said. Additionally, the NRC began an inspection of water pumps that help cool the reactor, an NRC spokeswoman said. Some pumps are designed to switch off after a set period of time after detecting an undervoltage to prevent damage, then must be manually restarted. But some of those pumps shut down and restarted on their own after the outage. She said there was no danger because the plant has multiple backup pumps, but the NRC wants all pumps to perform properly.
Source: http://www.pantagraph.com/news/state-and-regional/illinois/nrc-inspecting-water-pumps-at-stalled-us-reactor/article_da6e6c7c-5720-5431-8137-3d237afd7d43.html

8. *January 31, Biloxi Sun Herald* – (California) **San Onofre Nuclear Generating Station operators perform precautionary shutdown of reactor unit.** Southern California Edison, operator of the San Onofre Nuclear Generating Station in San Diego County, California, began a precautionary shutdown of the plant's Unit 3 reactor January 31 because sensors installed for this purpose detected a possible leak in one of the unit's steam generator tubes. The potential leak posed no imminent danger to the public or plant workers. There was no release to the atmosphere. San Onofre personnel will evaluate the cause of the leak and the steps required to repair it and resume operations.
Source: http://www.sunherald.com/2012/01/31/3722590/san-onofre-nuclear-generating.html

9. *January 31, Reuters* – (National) **NRC wants U.S. nuclear operators to adopt new seismic model.** The Nuclear Regulatory Commission (NRC) said January 31 that the agency wants nuclear plant operators in the central and eastern United States to use a new seismic model to reassess the potential for earthquakes in their area. A NRC study focused on this area because it is considered a "stable continental region" where big earthquakes are rare. The study, which gathered historical earthquake and geological data from 1568 through 2008, determined the largest potential earthquakes in the eastern and central parts of the country could occur near New Madrid, Missouri, and also in Charleston, South Carolina, where large magnitude seismic activity has occurred in the past.

Source: http://www.reuters.com/article/2012/01/31/us-utilities-nrc-earthquakes-idUSTRE80U1OS20120131

[Return to top]

Critical Manufacturing Sector

10. *January 31, U.S. Consumer Product Safety Commission* – (National) **Arctic Cat recalls snowmobiles due to crash hazard.** Arctic Cat announced January 31 the recall of about 19,000 model year 2012 F, XF, and M model snowmobiles. The lower steering tie-rod attachment can loosen and cause loss of steering control, posing a crash hazard. Arctic Cat has received four reports of incidents, including one complete loss of steering control. No injuries have been reported. Consumers should immediately stop using these snowmobiles and contact their local Arctic Cat snowmobile dealer to schedule a free inspection and repair. Arctic Cat has notified owners of these snowmobiles directly by mail.
    Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12716.html

11. *January 31, U.S. Department of Labor* – (Texas) **U.S. Labor Department's OSHA cites manufacturer for exposing workers to multiple safety hazards at Euless, Texas facility.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) January 31 cited KGP Group Inc., doing business as SpeQtrum Prepress Production Services, for 14 serious and one other-than-serious safety violation at its facility in Euless, Texas. SpeQtrum manufactures printing plates and cutting dies. The OSHA's Fort Worth Area Office initiated an inspection December 2 under the agency's Site-Specific Targeting Program, which focuses enforcement efforts on industries with high injury and illness rates. Proposed penalties totaled $44,800. The serious violations involved failing to: keep exit areas unobstructed; properly store compressed gas cylinders; provide proper machine guarding; ensure forklifts were properly serviced and maintained; provide forklift operator training; address electrical wiring deficiencies; mount fire extinguishers.
    Source:
    http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=21720

12. *January 31, MLive.com* – (Michigan) **Fire chief: Cannon-Muskegon explosion caused by 'breached' furnace liner.** Molten metal that came in contact with a water-filled copper coil was the cause of a January 30 explosion at the Cannon-Muskegon Corp. foundry in Norton Shores, Michigan, a fire official said. The Norton Shores fire chief said something caused a ceramic furnace liner to be "breached," which allowed molten metal to come in contact with the copper coil. The explosion inside the foundry forced the 35 employees working at the time out of a small portion of the building. Ten were near the furnace when it exploded.
    Source: http://www.mlive.com/news/muskegon/index.ssf/2012/01/post_188.html

For another story, see item **1**

[Return to top]

Defense Industrial Base Sector

13. *January 31, Ars Technica* – (International) **Fake Windows updater targets government contractors, stealing sensitive data.** Two security companies released a joint report January 31 describing an ongoing series of attacks against government contractors that have been occurring since at least early 2009. According to the vendors Seculert and Zscaler, attackers are sending firms phishing e-mails with fake invitations to conferences, often in the form of PDF files that exploit flaws in Adobe Reader. The file installs what the vendors call an "MSUpdater" trojan that poses as a legitimate Windows Update process. In reality, the trojan is a remote access tool that can steal data from a company's network for as long as the breach remains undiscovered. "Foreign and domestic (United States) companies with intellectual property dealing in aero/geospace and defense seem to be some of the recent industries targeted in these attacks," the report states, without identifying specific attack targets. The vendors believe the attacks are either state-sponsored or perpetrated by a high-profile group of attackers, but they have not yet been able to determine their identities, according to Seculert's CTO.
Source: http://arstechnica.com/business/news/2012/01/fake-windows-updater-targets-government-contractors-stealing-sensitive-data.ars

[Return to top]

Banking and Finance Sector

14. *February 1, BBC News* – (International) **Four men admit London Stock Exchange bomb plot.** Four men inspired by al-Qa'ida admitted planning to detonate a bomb at the London Stock Exchange, BBC News reported February 1. The men all pleaded guilty in court in England to engaging in conduct in preparation for acts of terrorism. The men, from London and Cardiff, were arrested in December 2010. Five other men linked to the plot pleaded guilty to other terrorism offenses and all nine will be sentenced the week of February 6. It emerged that those who targeted the London Stock Exchange wanted to send five mail bombs to various targets during the run up to Christmas 2010, and discussed launching a "Mumbai-style" atrocity. A hand-written target list discovered at the home of one of the men listed the names and addresses of London's mayor, two rabbis, the U.S. embassy, and the stock exchange. The conspiracy was stopped by undercover anti-terror police before firm dates could be set for attacks. The terrorists met because of their membership of various radical groups and stayed in touch over the Internet, through mobile phones, and at specially arranged meetings. The quartet talked about leaving homemade bombs in the toilets of their city's pubs and discussed traveling abroad for terror training.
Source: http://www.bbc.co.uk/news/uk-16833032

15. *February 1, Help Net Security* – (International) **Malware redirects bank phone calls to attackers.** Trusteer has discovered a concerning development in new configurations of Ice IX, a modified variant of the ZeuS financial malware platform, that are targeting

online banking customers in the United Kingdom (UK) and United States. "In addition to stealing bank account data, these Ice IX configurations are capturing information on telephone accounts belonging to the victims ... allow[ing] attackers to divert calls from the bank intended for their customer to attacker controlled phone numbers," the chief technology officer (CTO) of Trusteer said. He believes "the fraudsters are executing fraudulent transactions using the stolen credentials and redirecting the bank's post-transaction verification phone calls to professional criminal caller services that approve the transactions." In one captured attack, at login the malware steals the victim's user ID and password, memorable information/secret question answer, date of birth, and account balance. Next, the victim is asked to update phone numbers and select the name of their service provider from a drop-down list. To enable the attacker to modify phone service settings, the victim is then asked by the malware to submit telephone account number. The fraudsters justify this request by stating this data is required as a part of verification process caused by "a malfunction of the bank's anti-fraud system with its landline phone service provider."
Source: http://www.net-security.org/malware_news.php?id=1984

16. *February 1, H Security* – (International) **Hacker extracts RFID credit card details.** The widespread use, especially in U.S. credit cards, of radio frequency identification (RFID) chips which can be read through clothing or wallets for contactless payments can lead to cards being read without the owners knowledge or permission, H Security reported February 1. Forbes reported January 30 that a hacker at the Shmoocon security conference in Washington D.C. demonstrated the ability to read data on RFID chipped credit cards and make a payment that had not been authorized by the card owner. With about 100 million RFID cards issued, this could now be done without card owners handing over their cards. No security measures such as card reader authentication are in place. However, the RFID data does not include the three-digit CVV number printed on the back of the card that is usually required when making an online transaction. Instead, the chip issues a one-time CVV that is only valid for one transaction. Using this CVV repeatedly will cause the card to be blocked. In the United States, Visa markets RFID credit cards as payWave, and in the United Kingdom (UK) as Contactless by Visa. Mastercard markets their RFID credit cards as Paypass in the United States and UK.
Source: http://www.h-online.com/security/news/item/Hacker-extracts-RFID-credit-card-details-1425974.html

17. *January 31, Infosecurity* – (National) **Trymedia breach exposes credit card numbers of 12,000 digital game customers.** Trymedia's ActiveStore Web-based storefront application, which processes digital game purchases made by customers on its partners' Web sites, was recently breached, exposing credit card numbers and other personal information of more than 12,000 customers, Infosecurity reported January 31. Trymedia told the New Hampshire Attorney General's Office it believes hackers were able to obtain credit card numbers, expiration dates, security codes, and postal and e-mail addresses to optional users accounts for transactions between November 4 and December 2. Trymedia said it would notify the 12,456 customers affected by postal mail about the potential breach and offer to provide a 12-month subscription to a credit-monitoring and identity-theft protection product.

Source: http://www.infosecurity-us.com/view/23586/trymedia-breach-exposes-credit-card-numbers-of-12000-digital-game-customers/

18. *January 31, Associated Press* – (International) **Hackers attack large Brazilian Bank.** A group of Internet hackers said January 31 it took down the Web site of Brazil's second largest private sector bank, one day after it did the same with the country's largest private bank. The group that calls itself "Anonymous Brasil" said on Twitter: "Attention sailors: Target hit! The http://bradesco.com.br is sinking. TANGO DOWN." Banco Bradesco SA said in a statement its site suffered "momentary interruptions," due to high traffic, but that it was never forced offline. The group said on Twitter its attacks were a protest against corruption and would continue for at least a week. The group attacked the website of Itau Unibanco Banco Multiplo SA , Brazil's largest private sector bank, January 30, saying it was the first of several such attacks. That bank said in a statement its site was offline for part of the day, but that it was re-established after the problem was detected.
Source: http://techland.time.com/2012/01/31/hackers-attack-large-brazilian-bank/

19. *January 31, U.S. Securities and Exchange Commission* – (Illinois; New York) **SEC charges brothers with short selling violations.** The U.S. Securities and Exchange Commission (SEC) January 31 charged two brothers living in Chicago and New York with naked short selling for failing to locate and deliver shares involved in short sales to broker-dealers. While short selling is legal, SEC rules require short sellers to locate shares to borrow before selling them short, and they must deliver the securities by a specified date. According to the SEC's order instituting administrative proceedings against the brothers, they generated more than $17 million in ill-gotten gains. The SEC's alleges one of the men engaged in illegal naked short sales while working as a broker-dealer and later as the principal trader at a now defunct Chicago-based broker-dealer. His brother conducted illegal naked short sales while trading through Golden Anchor Trading II LLC, a New York-based broker-dealer, which the SEC has also charged. According to the order, the brothers engaged in two types of transactions from July 2006 to July 2007. The first type of transaction – a "reverse conversion" or "reversal" – involves selling stock short and simultaneously selling a put option and buying a call option on the stock. The second type was a stock and option combination that created the illusion he party subject to a close-out obligation had satisfied that obligation by buying the same kind and quantity of securities it had sold short. However, the brothers knew or had reason to know the shares purchased in the sham transactions would never be delivered because they were purchased from another seller who also did not have the stock.
Source: http://www.sec.gov/news/press/2012/2012-22.htm

20. *January 31, Associated Press* – (National) **IRS says federal sweep against identity theft targets 105 people in 23 states in past week.** The federal government has swooped down on 105 people in 23 states in the past week as part of a nationwide crackdown on identity theft and tax refund fraud timed to warn cheats to beware this tax season, the Internal Revenue Service (IRS) said January 31. The sweep, which ranged from Alaska to Florida and included 80 complaints and indictments and 58 arrests, has already produced a handful of guilty pleas and sentencings. Besides the

IRS, the Justice Department's Tax Division, the Postal Service, and local U.S. attorney's offices were involved after investigations that lasted months and, in some cases, years. In 2011, the agency said it found 260,000 income tax returns with confirmed attempts at identity fraud and blocked the payment of $1.4 billion worth of refunds. Over the past week, IRS officials have also visited 150 money services businesses to see if they are involved in identity theft or filing for bogus refunds. This sweep was conducted in nine metropolitan areas the IRS considers high risk: Atlanta; Birmingham, Alabama.; Chicago; Los Angeles; Miami; New York; Phoenix; Tampa, Florida; and Washington, D.C. In addition, the agency is auditing more than 250 check-cashing operations around the United States, in part to try to spot any identity theft activity. The IRS's deputy commissioner for services and enforcement said in 2012 the IRS installed new filters on its computers in an attempt to spot identify fraud before the agency pays a phony refund.
Source: http://www.chicagotribune.com/sns-ap-us-irs-identity-theft,0,585346.story

21. *January 31, Boulder Daily Camera* – (Colorado) **FBI: Two Boulder bank robberies committed by 'Face Off Bandit'.** The FBI now believes that two bank robberies this winter in Boulder, Colorado, were committed by the same robber, who they believe also targeted banks in Golden and Thornton, the Boulder Daily Camera reported January 31. The FBI said a man they are calling the "Face Off Bandit" is likely responsible for robberies at a Great Western Bank December 16, and a First Bank January 19 in Boulder. Investigators also believe the robber hit a Wells Fargo Bank in Golden in September, and a Key Bank in Thornton in November. In all four cases, the suspect entered the banks with some sort of fake facial hair, presented a note demanding money, and left. In one of the Boulder robberies, police believe he also used a hat with hair attached to it.
Source: http://www.dailycamera.com/boulder-county-news/ci_19862212

22. *January 30, U.S. Securities and Exchange Commission* – (Arizona; International) **Relationship partner at accounting firm charged with fraud and barred for five years; former Syntax-Brillian Corp. executive ordered to pay more than $48 million for insider trading and financial fraud.** The U.S. Securities and Exchange Commission (SEC) January 30 filed settled charges against a partner at an accounting firm for aiding and abetting a fraudulent revenue recognition scheme at Syntax-Brillian Corporation, a developer of high-definition LCD televisions. In addition, a district court judge in Arizona January 12 entered a default judgment against the chief procurement officer and a director of Syntax. The court permanently enjoined the director from future violations of the antifraud, reporting, books and records, internal controls, and misrepresentation to auditor provisions of securities laws, and ordered him to pay disgorgement, prejudgment interest, an insider trading penalty, and a civil penalty totaling more than $48 millions for his role in the scheme. He was also permanently barred from serving as an officer or director of a publicly traded company. As alleged in the SEC's complaint against the director, from at least June 2006 through April 2008, he and other Syntax senior executives engaged in a complex scheme to overstate Syntax's revenues and earnings and artificially inflate its stock price. The scheme included the creation of fictitious sales and shipping documents and coordinating the circular transfer of funds among and between Syntax, its primary

manufacturer in Taiwan, and its purported distributor in Hong Kong. In its complaint against the partner, the SEC alleged he instructed Syntax executives on how to create a backdated distribution agreement to assist them in improperly recognizing revenue.
Source:
http://www.sec.gov/litigation/litreleases/2012/lr22243.htm?utm_medium=twitter&utm_source=twitterfeed

For another story, see item **NaN**

[Return to top]

Transportation Sector

23. *February 1, Detroit Free Press* – (Michigan) **Amtrak train smashes into semi near Jackson.** A Chicago-bound Amtrak train smashed into a semi near Jackson, Michigan, February 1, injuring six people and forcing one of the train's engines to derail, police said. None of the injuries –- the train was carrying 71 passengers total –- was considered life threatening, said a spokesman for the Blackman/Leoni Public Safety Department, which serves two townships near Jackson. The passengers and the driver of the semi were transported to a local hospital, he said. The truck driver told authorities he was hauling a lowboy trailer that was too low to make it across tracks on North Portage Road near East Michigan Avenue in Leoni Township. The train struck the truck around 8:19 a.m. The spokesman said the train could have been traveling in excess of 50 mph. The Wolverine Line 351 train, with two locomotives and six rail cars, was traveling from Pontiac to Chicago, Amtrak said. There were five crew members aboard. Amtrak said the engine was on its side at the scene, and the first two cars came off the rails. Amtrak said it would suspend service across central Michigan for several hours, and would arrange alternate transportation for passengers on the crashed train and other Wolverine line trains.
Source: http://www.freep.com/article/20120201/NEWS06/120201017/Amtrak-train-smashes-into-semi-near-Jackson?odyssey=tab|topnews|text|FRONTPAGE

24. *February 1, Trenton Times* – (New Jersey) **Gunshots, a killing and a highway in Trenton shut down for 16 hours.** Police, January 31 identified a Trenton, New Jersey man as the victim of a fatal drive-by shooting January 30 on Route 29, in which the assailants let fly a hail of bullets on the open highway before crashing their car and fleeing on foot. The busy highway was shut down for more than 16 hours overnight January 30-31 as city detectives scoured the scene, a few hundred yards from the statehouse building collecting evidence. The victim was riding in a car driving north on 29 shortly before 6:30 p.m. January 30 when a second car carrying the suspects pulled even, and they opened fire, a police spokesman said. That car continued up the highway before crashing near the Memorial Drive on-ramp. The suspects' car had a minor accident with another vehicle. The suspects fled their vehicle. Despite a large-scale police operation that included the closure of a significant portion of 29, no arrests had been made as of January 31. The closure caused delays for thousands traveling to Trenton. The northbound lanes of 29 were closed between Calhoun Street and Cass Street until 11 a.m. The state department of transportation reported 90 minute delays on

Interstates 195 and 295 as traffic was detoured onto Route 129.
Source:
http://www.nj.com/mercer/index.ssf/2012/02/police_identify_trenton_man_as.html

25. *January 31, Reuters* – (Tennessee) **Rockslide shuts highway in Tennessee, causing massive detour.** A rockslide forced Tennessee to close a 1-mile section of westbound Interstate 40 near the border with North Carolina for at least 2 weeks, forcing drivers to take a 53-mile detour, transportation officials said February 1. The early morning slide included a rock 40-feet long, 40-feet high and 15-feet thick that weighed about 1,500 tons, said a spokesman for the Tennessee Department of Transportation. The 1-mile stretch will remain shut until debris can be removed and inspectors can make sure the rock walls are stable. Meanwhile, westbound drivers will be directed along a 53-mile detour starting near Asheville, North Carolina, into Tennessee. A rockslide in the same area in 2009 forced eastbound lanes to be shut for 6 months.
Source: http://www.chicagotribune.com/news/sns-rt-us-tennessee-rockslidetre80u29t-20120131,0,4895702.story

26. *January 31, Associated Press* – (Florida) **11th victim found days after deadly crash on I-75.** The body of an eleventh person has been found in a pickup truck days after a deadly pileup on Interstate 75, the Florida Highway Patrol (FHP) said. The victim was inside a Dodge pickup truck that crashed into a tractor trailer as it traveled south early January 29, authorities determined January 31. Authorities closed the busy six-lane highway just after midnight January 29 because a mix of fog and smoke from a nearby brush fire made visibility difficult. The road was reopened about 3 hours later after the FHP determined conditions had improved. The first pileup occurred a short time later. Florida officials said they are willing to review their protocols in determining when to shut down — and reopen — a major highway. Officials said the decision to close a road is made by a FHP supervisor, who relies on feedback from troopers who assess road conditions. They use information and forecasts from the National Weather Service (NWS). A key piece of data is an index estimating the humidity and smoke dispersion on a scale of 1 to 10. If the score is 7 or higher, the FHP's protocol is to close the road. The index score for early January 29 had been forecast to be a 6 in the four-county region that includes the crash site, according to the NWS.
Source: http://www.bellinghamherald.com/2012/01/31/2373775/7th-victim-in-deadly-fla-highway.html

For more stories, see items **5** and **57**

[Return to top]

Postal and Shipping Sector

27. *January 31, KAKE 10 Wichita* – (Kansas) **Keep an eye on your mailbox.** Local authorities are working with the U.S. Postal Service to stop mail thefts in South Central Kansas, KAKE 10 Wichita reported January 31. Butler, Sedgwick, and Cowley Counties all reported mail thefts in the last few weeks. A Cowley County homeowner said someone stole her mail the week of January 23. She came home to find her

mailbox opened and empty. The Cowley County sheriff said thieves are looking for any kind of financial information they can find.
Source:
http://www.kake.com/news/headlines/Keep_Watch_On_Your_Mailbox_138420819.html

[Return to top]

Agriculture and Food Sector

28. *February 1, Food Safety News* – (Pennsylvania; Maryland) **20 Campylobacter cases now linked to raw milk dairy.** Pennsylvania health authorities said January 31 the number of confirmed cases in an outbreak of Campylobacter infection rose to 20 — 16 from that state and 4 from Maryland. All of the people who are sick consumed unpasteurized milk from The Family Cow dairy in the Chambersburg area, according to a report in the Harrisburg Patriot-News. Pennsylvania and Maryland departments of health issued a health alert January 27 advising people to discard any products purchased from the farm after January 1. The Pennsylvania Department of Agriculture is testing samples collected from the dairy. Results were expected February 1 or 2, according to a department spokeswoman. The dairy voluntarily stopped selling milk, but the owner said an independent lab retained by the dairy tested samples taken January 27 and reported that batch of milk was free of pathogens. News reports said those stricken with campylobacteriosis began getting sick about 2 weeks ago. The incubation period for Campylobacter can range from 2 to 10 days.
Source: http://www.foodsafetynews.com/2012/02/20-campylobacter-cases-linked-to-raw-milk-dairy/

29. *February 1, Food Safety News* – (National) **Allergen alert: Rice crackers with egg.** Gemini Food Corporation of City of Industry, California, and Tong Enterprises of Hayward, California, are recalling certain Bin-Bin crackers because they contain egg, an allergen not listed on the label, Food Safety News reported February 1. There was one allergic reaction reported in connection with the rice crackers. The recall is for 5.3-ounce Bin-Bin Snow Rice Crackers and for 15.8-ounce Bin-Bin Rice Crackers. The crackers were distributed to grocery stores by Gemini Food Corporation nationwide, and by Tong Enterprises to grocery stores in California between January 1, 2011 and January 31, 2012.
Source: http://www.foodsafetynews.com/2012/02/allergen-alert-rice-crackers-with-egg/

30. *February 1, Food Safety News* – (National) **Allergen alert: Milk in peanut butter candy.** How Sweet It Is Fudge and Candy Company is recalling and correcting the labels of its 32-count packages of Peanut Butter Buckeye and Peanut Butter Smoothie candy because they contain milk, an allergen not listed as an ingredient, Food Safety News reported February 1. The recall was initiated January 25 after a consumer with a milk allergy ate a Peanut Butter Buckeye and complained to the company. The company said it has since corrected the label, but is also advising consumers who purchased the candy earlier that the product does contain a milk ingredient. The recalled boxes were distributed from December 1, 2011 to January 23, 2012 to

wholesale distributors, service stations, and convenience stores in Michigan, Pennsylvania, Ohio, Tennessee, Indiana, Virginia, and New York.
Source: http://www.foodsafetynews.com/2012/02/allergen-alert-milk-in-peanut-butter-candy/

31. *January 31, Food Safety News* – (National) **Allergen alert: Bridge mix in chocolate raisin packaging.** Walgreen Co. is recalling certain lots of packages with chocolate-covered raisin labels because they may instead contain bridge mix, which includes peanuts, almonds, and soy, allergens not listed as ingredients, Food Safety News reported January 31. After receiving a consumer complaint of an allergic reaction, Walgreen said it learned the product manufacturer, GKI Foods of Brighton, Michigan, mistakenly packaged bridge mix with chocolate-covered raisin labeling. The recalled packages were distributed through Walgreen distribution centers in Arizona, Connecticut, and California, and to Walgreens retail stores in the Northeastern and Western United States.
Source: http://www.foodsafetynews.com/2012/01/allergen-alert-bridge-mix-in-chocolate-raisin-packaging/

For another story, see item **57**

[Return to top]

Water Sector

32. *February 1, Associated Press* – (Nebraska) **Plant ends need for bottled water.** More than a decade after being notified of having the highest uranium levels of any Nebraska town, Clarks has completed a permanent solution, the Associated Press reported February 1. A new $1.04 million water treatment plant went online January 11. The mayor said the state notified the village in late 2000 that Clarks' water supply had 220 parts per billion (ppb) of uranium, which can cause kidney failure when very high concentrations are consumed long term. In 2003, the Environmental Protection Agency revised its radionuclides rule and decided the standard for uranium should be 30 ppb. Clarks began testing water from existing wells in a 3-mile radius of the village in June 2003. New wells were drilled in April 2005, with a water line constructed to the village at a cost of about $450,000. But 3 months later, uranium started showing up again. This time, it was at much lower rates, between 48 and 68 ppb. In 2007, the village determined the only long-term solution was to remove the uranium.
Source: http://www.omaha.com/article/20120201/NEWS01/702019889/-1

33. *January 31, WBNS 10 Columbus* – (Ohio) **Town's water well tests positive for E. coli.** A city-wide boil advisory was sent out January 30 after one of Greenfield, Ohio's eight water wells tested positive for E. coli bacteria. The advisory was originally issued for a six-block portion of the village, but was later expanded to the entire village. The source of the bacteria was not immediately known. Some village residents criticized officials for not getting the word out soon enough. Officials said the well that tested positive for bacteria was shut down. The boil advisory was expected to last at least 7

days.
Source: http://www.10tv.com/content/stories/2012/01/31/greenfield-boil-advisory.html

34. *January 31, Lafayette Journal Courier* – (Indiana) **Future of Durkee's Run destined to be clearer.** The Lafayette, Indiana Board of Works contracted a civil engineering firm January 31 for assistance with the city's project to improve drainage along Durkee's Run. The contract will be used to separate storm and sanitary sewers along the run, a city engineer said January 31. The project, expected to begin in 2013, would prevent household sewage and commercial wastewater from entering the run. Currently, the combined sanitary and storm sewers overflow during heavy rains, sending untreated sewage into the run, and the Wabash River. When the project is completed, stormwater and sanitary sewage will be directed to the water treatment plant; Durkee's Run will be fed only by runoff from stormwater, the engineer said. Currently, storm sewers along Earl Avenue are insufficient to handle heavy rain, causing water to back up on Earl Avenue and U.S. 52/Sagamore Parkway.
Source: http://www.jconline.com/article/20120201/NEWS/202010306/Future-Durkee-s-Run-destined-clearer?odyssey=mod|newswell|text|FRONTPAGE|s

For another story, see item **53**

[Return to top]

Public Health and Healthcare Sector

35. *February 1, Associated Press* – (National) **Pfizer recalls 1M birth control packs after mixup.** Pfizer Inc. is recalling 1 million packets of birth control pills due to a packaging error that could raise the risk of an accidental pregnancy by leaving women with an inadequate dose. Pfizer found some packets of the drugs had too many active tablets, while others had too few. Oral birth control products use a series of 21 hormone tablets and 7 inactive sugar tablets to regulate the menstrual period while providing contraception. The problem affects 14 lots of Lo/Ovral-28 tablets and 14 lots of generic Norgestrel and Ethinyl Estradiol tablets. Both products are manufactured by Pfizer and marketed in the United States by Akrimax Rx Products under the Akrimax Pharmaceuticals brand. A Pfizer spokeswoman said the problem was caused by mechanical and visual inspection failures on the packaging line. She said the problem has been corrected. Patients with the affected lot numbers should return them to the pharmacy. The affected packets have expiration dates ranging between July 31, 2013, and March 31, 2014. The drugs were distributed to warehouses, clinics and retail pharmacies throughout the United States.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5h7oszk1RBsQuNjBK_8wMMkiqKDaA?docId=0cc71c595a72410a8375533c9c5eb70c

36. *January 31, Associated Press* – (Indiana) **N. Ind. hospital says some records, including Social Security numbers, may have been breached.** Indiana University Health Goshen Hospital in Goshen, Indiana will notify more than 12,800 job applicants and patients that their personal information may have been obtained illegally through a

computer virus. A hospital spokeswoman said the virus was discovered December 22. An Internet security company hired by the hospital was not able to determine whether any data was accessed, just that someone tried to access it. The hospital is sending letters to 12,374 people who applied for hospital jobs in the past several years, and fewer than 500 patients who pre-registered for outpatient procedures over the Internet that their names, addresses and Social Security numbers may have been compromised. The hospital is also offering to pay for 1 year of credit monitoring for all of the people affected.
Source:
http://www.greenfieldreporter.com/view/story/239993f76f454deb9b2a29e0ab244ecf/IN--Hospital-Records-Breach/

[Return to top]

Government Facilities Sector

37. *February 1, The Register* – (International) **Romanian cops cuff suspected serial hacker TinKode.** Romanian police arrested a man suspected of breaking into the Web sites of NASA and the Pentagon in a series of high-profile hack attacks, The Register reported February 1. The man, 20, from Timisoara in Romania, is accused of publishing details of the SQL injection vulnerabilities discovered on the targeted Web sites under the hacker handle TinKode. The Romanian Directorate for Investigating Organized Crime and Terrorism further alleged the man, an IT student, sold hacking tools from his personal site. TinKode bragged about breaking into the British Royal Navy's Web site in November 2010 and making off with site passwords. Other attacks claimed by TinKode included breaking into the MySQL site (using a SQL injection vulnerability), and the European Space Agency. These alleged targets fail to appear on the rap sheet, which concentrates on the NASA hack and an assault on U.S. Army systems that allegedly resulted in the extraction of confidential data. Investigating officers from the FBI and NASA took part in the investigation that led to his arrest. The motive for all of the attacks seems to be to claim high-profile scalps and obtain bragging rights in the process.
Source: http://www.theregister.co.uk/2012/02/01/tinkode_nasa_hack_suspect_cuffed/

38. *February 1, Portland Oregonian* – (Oregon) **Environmental penalties for Umatilla Chemical Depot total nearly $800,000 since 1999.** Oregon environmental regulators announced a $46,800 penalty against the operators of the Umatilla Chemical Depot in Umatilla, January 31, bringing total depot penalties to nearly $800,000 since 1999. Washington Demilitarization Co., a division of URS Corp., is in charge of incineration at the U.S. Army's depot, which finished destroying 3,720 tons of mustard "blister" agent and sarin and VX nerve agents in October. The four violations announced January 31 occurred in June and September, the Oregon Department of Environmental Quality (DEQ) said. They involved excess carbon monoxide emissions during mustard agent incineration, air monitoring failures, and improper maintenance of monitoring equipment. As with the violations in 24 prior penalties since 1999, none of the latest problems harmed the environment or public health, the DEQ said. A protocol officer for Washington Demilitarization said backup controls and monitoring systems would

have caught emissions of serious concern. None of the emissions reached workers, he said.
Source: http://www.oregonlive.com/environment/index.ssf/2012/01/environmental_penalties_for_um.html

39. *January 31, Skidmore News* – (New York) **Results from initial Starbuck testing released.** On January 31, the dean of student affairs at Skidmore College in Saratoga Springs, New York, released a statement to the student body reporting initial testing in the Starbuck building had been completed and that the results indicated no abnormal gas levels. Although the nature of the health concerns which led to the evacuation of 50 employees from the building have yet to be disclosed to the student body, the statement revealed that tests for radon, carbon dioxide, carbon monoxide, and volatile organic compounds were identified as being within or below recommended ranges. No detectable levels of formaldehyde were identified. An industrial hygienist consultant from ATC Associates Inc., who the college employed to investigate these health concerns, found mold in one room and recommended that the college take steps to alleviate the problem. College officials plan to take action once all employees have fully evacuated the building, which is scheduled to occur by mid-February.
Source: http://www.skidmorenews.com/news/results-from-initial-starbuck-testing-released-1.2759090#.TylkS4F7eEB

40. *January 31, Associated Press* – (Utah) **Suspect in Utah school bomb plot charged.** Authorities filed charges against a 16-year-old boy accused in a plot to detonate a bomb at a Utah high school, the Associated Press reported January 31. Police said the teenager, along with an 18-year-old, planned to bomb an assembly at Roy High School, in Roy, Utah. Both were arrested the week of January 23. The 18-year-old has been charged with possession of a weapon of mass destruction. Prosecutors January 31 charged the 16-year-old with the same count in juvenile court, but have filed a motion seeking to try him as an adult. Police said the plot was foiled when another student came forward after receiving ominous text messages from one of the suspects hinting at their plan.
Source: http://www.cachevalleydaily.com/news/local/Suspect-in-Utah-school-bomb-plot-charged-138445339.html

For another story, see item **14**

[Return to top]

Emergency Services Sector

41. *February 1, WLUK 11 Green Bay* – (Wisconsin) **Thefts suspected from Marinette ambulances.** The president of Marinette's Emergency Rescue Squad Inc. said four bags containing $600 worth of CPR equipment were stolen from Marinette, Wisconsin area ambulances, WLUK 11 Green Bay reported February 1. He said the bags were taken from ambulances parked in driveways of on-call volunteers. He believes people are taking the bags thinking they are going to score drugs. The ambulances sit in the

volunteers' driveways unlocked. With the suspected thefts, the rescue group might change protocol. Two of the four missing bags were found empty in waters around Marinette. Some of the equipment was found scattered along the shoreline, however it was too waterlogged to be salvaged.
Source: http://www.fox11online.com/dpp/news/local/north_counties/Thefts-suspected-from-Marinette-ambulances

42. *February 1, KVUE 24 Austin* – (Texas) **Hutto man arrested for impersonating police officer.** A central Texas man has been arrested for impersonating a police officer. He was arrested January 19 after Williamson County constables were tipped off by other peace officers. The suspect was the vice president of Emergency Lighting Vehicle Servicesof Pflugerville. It is a business that would help equip law enforcement agencies with lighting and other special equipment for the vehicles. Authorities said the man was involved in at least five incidents, and possibly many more, where he tried to pass himself off as a peace officer. Investigators said the suspect has never been a police office in Texas. In fact, he is a convicted felon in Travis County and is not allowed to possess a weapon until 2015.
Source: http://www.kvue.com/news/Hutto-man-arrested-for-impersonating-police-officer-138443319.html

43. *February 1, KNBC 4 Los Angeles* – (California) **Sheriff station firebomb attack caught on video.** Santa Barbara, California sheriff's detectives arrested a 23-year-old, Isla Vista man in connection with allegedly throwing a Molotov cocktail firebomb at the Isla Vista Foot Patrol sheriff's station January 1. KNBC 4 Los Angeles reported February 1 the suspect was being held on $250,000 bail at the Santa Barbara County jail on suspicion of felony arson of an inhabited dwelling. The attack was caught on video by sheriff's surveillance cameras. A similar attack November 15, was also caught on video where a man could be seen throwing two Molotov cocktails. The suspect in the January 1 attack was taken into custody January 25, according to a news release provided by the Santa Barbara's sheriff's office. The November 15 case remains unsolved and is still under investigation.
Source: http://www.nbclosangeles.com/news/local/Sheriff-Station-Firebomb-Attack-Caught-on-Video-138445259.html

44. *January 30, Houston Chronicle* – (Texas) **Baytown man sentenced for smuggling AK-47 tied to fatal shooting of ICE agent.** A Baytown, Texas man was sentenced to more than 8 years in prison for illegally exporting firearms to Mexico, including an AK-47-like weapon, found at the scene where a U.S. federal agent was shot to death by members of the Zetas drug cartel, authorities announced January 30. He pleaded guilty to the charge at the federal courthouse in Houston. He could not legally buy firearms because he was already on deferred adjudication for two felony drug offenses from Harris County, according to a statement released by prosecutors. He recruited individuals known as straw buyers to buy numerous AK-47-like guns, the statement continues. He would have the serial numbers obliterated from the guns before they were smuggled to Mexico for use by the Zetas. Among the guns, prosecutors said he sent to Mexico was one used in the February 2011 attack that killed an Immigration and Customs Enforcement agent and wounded another ICE agent. The gun was bought at

J&J's Pawn shop, in Beaumont.
Source: http://www.chron.com/news/houston-texas/article/Baytown-man-sentenced-for-smuggling-AK-47-tied-to-2848835.php

For more stories, see items **26** and **52**

[Return to top]

Information Technology Sector

45. *February 1, H Security* – (International) **Mozilla closes critical holes in Firefox, Thunderbird and SeaMonkey.** Following the release of new versions of its open source Firefox Web browser, Thunderbird e-mail client, and SeaMonkey suite, Mozilla detailed the security fixes included in each of the updates. According to the project's Security Center page for Firefox, version 10.0 closes a total of eight security holes in the browser, five of which are rated as "Critical" by Mozilla. The critical issues include an exploitable crash when processing a malformed embedded XSLT stylesheet, potential memory corruption when decoding Ogg Vorbis files, XPConnect security checks being bypassed by frame scripts, a use after free error in child nodes from nsDOMAttribute, and various memory safety hazards. These vulnerabilities could be exploited remotely by an attacker to, for example, execute arbitrary code on a victim's system. Additionally, Firefox 10 closes two "High" impact issues that could lead to information disclosure or an attacker violating the HTML5 frame navigation policy by replacing a sub-frame for phishing attacks. A moderate severity bug when exporting a user's Firefox Sync key to a "Firefox Recovery Key.html" file that caused it to be saved with incorrect permissions was also fixed.
Source: http://www.h-online.com/security/news/item/Mozilla-closes-critical-holes-in-Firefox-Thunderbird-and-SeaMonkey-1426048.html

46. *January 31, H Security* – (International) **Security hole in Sudo's debug option closed.** A hole in the sudo command's debug options was fixed by the developers, H Security reported January 31. The problem, discovered by joernchen of phenoelit, affects sudo versions 1.8.0 to 1.8.3p1. The sudo command is used extensively by Linux distributions, Mac OS X, and other Unix operating systems to allow users to execute commands with super user privileges without logging in as root. The security hole appeared in version 1.8.0 when a new simple debugging option was added.
Source: http://www.h-online.com/security/news/item/Security-hole-in-Sudo-s-debug-option-closed-1425163.html

47. *January 31, Threatpost* – (International) **Kelihos botnet resurfaces.** The Kelihos botnet, which researchers at Kaspersky Lab and Microsoft disrupted last fall by sinkholing the control channel, sprung back to life and is using only slightly different versions of the original malware and controller list, Threatpost reported January 31. In late September, researchers from Kaspersky and Microsoft worked together on a coordinated takedown of the botnet, which involved sinkholing. This tactic involves researchers directing bots on infected computers to contact a server they control, rather than one controlled by the attackers. At the time of the takedown, a Kapersky

researcher said the sinkholing was not a permanent answer because the peers in the network would eventually begin communicating with other controllers and the sinkhole peer would lose its dominant position. The real solution would have been to push an update to the infected machines that removed the infection or disabled the bot, but there are legal and ethical obstacles to that course of action. What happened since the takedown in September is essentially what the researcher predicted. The Kelihos network reformed and is back in action, in only slightly modified form. The encryption routine the malware uses is slightly different from the old version, shuffling around the spots in which Blowfish and Triple-DES keys are used. The signing keys for certain components of the malware also changed.
Source: http://threatpost.com/en_us/blogs/kelihos-botnet-resurfaces-013112

48. *January 30, ZDNet* – (International) **Android malware makes use of steganography.** Security firm F-Secure released details on how Android malware makes use of steganography to hide the control parameters for rogue code. Steganography is the technique of hiding messages within something else, in this case, an icon file. F-Secure first suspected Android malware was making use of steganography when researchers came across a particular line of code. Further research revealed more code, and it soon became clear the image file being referenced was the icon file bundled with the rogue application. The hidden dtata is used to control how and when premium rate SMS messages are sent from the victim's handset, which is the primary purpose of the rogue application.
Source: http://www.zdnet.com/blog/hardware/android-malware-makes-use-of-steganography/17903

For more stories, see items **13**, **15**, **17**, and **18**

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

49. *February 1, Ardmore Daily Ardmoreite* – (Oklahoma) **Cable system target of vandalism.** The cable system in the Healdton, Oklahoma area has been the subject of controversy in recent months and a target of vandalism over the past week, the Ardmore Daily Ardmoreite reported February 1. The Healdton city manager said the head end station, located near Ratliff City, has been targeted since January 27. The resulting vandalism has caused damage to the cable and Internet in terms of financial loss and service."They moved the dish and cut some of the wires. It appears they scaled the fence," the city manager said. The Carter County Sheriff's Department is investigating the vandalism, which the city manager believes was a deliberate attempt

to sabotage the cable system. “They had to know what they were doing,” he said. “The average Joe wouldn’t know to go cut some of the wires and some of the lead wires. They also pulled the T1 wire which affected the Internet.” Reports of cable problems began filtering in January 27. Repairs were made, but another incident caused much more significant problems. “It happened somewhere between noon [January 30] and 6 a.m. January 31,” the city manager said. Based on information relayed to the city manager, it will take 16 to 20 hours of labor to get the system back up fully. There will be additional hours needed to realign some of the channels. He said any charges could also fall into the realm of the Federal Communications Commission.
Source: http://www.ardmoreite.com/news/x370663419/Cable-system-target-of-vandalism

For more stories, see items **15** and **48**

[Return to top]

Commercial Facilities Sector

50. *February 1, Associated Press* – (Virginia) **Three Rotunda fires under investigation.** Authorities are investigating a series of fires at an apartment building in Norfolk, Virginia, the Associated Press reported February 1. Three fires occurred at The Rotunda within a week. The latest was reported February 1. The Norfolk Fire-Rescue battalion chief said firefighters found trash burning in a hallway on the fifth floor. The sprinklers did not go off, and investigators were still on the scene conducting interviews hours after the fire. Decorations were removed from a door and set on fire January 25. Another fire occurred January 31 in a hallway closet. All three fires occurred on the building’s fifth floor. The battalion chief said the fires January 25 and February 1 are considered suspicious.
Source: http://www.fox43tv.com/dpps/news/local/norfolk/fires-at-apartment-under-investigation_4060079

51. *February 1, Associated Press* – (West Virginia) **Faulty pipe caused deadly W.Va. hotel gas leak.** Authorities in South Charleston, West Virginia are looking into how a pipe attached to a heating unit on a hotel’s indoor pool came apart, allowing deadly carbon monoxide fumes to escape. A Rhode Island construction worker was found dead in his fifth-floor room January 31 at the Holiday Inn Express and Suites along Corridor G. The fire captain said the pipe was supposed to remove exhaust from the natural gas unit and send it outdoors. He said the pipe somehow became detached near the hotel’s fourth floor, sending the colorless, odorless gas through several floors. He said the unit was repaired February 1. The hotel reopened to guests the night of January 31. The fire captain said another check of the hotel’s air quality was conducted “to give everybody a peace of mind.”
Source: http://www.stltoday.com/news/national/w-va-hotel-evacuated-after-guest-dies-sickened/article_5e006bef-6123-5d51-b7cc-15d2d58ee17b.html

52. *January 31, White Plains Journal News* – (New York) **70 in shelter displaced by 2 Yonkers fires; burned building to be leveled, owner says.** The eight-family

apartment building in Yonkers, New York, ravaged by a fire January 30 that left all of its tenants homeless will be torn down within 48 hours, the building's owner said January 31. Meanwhile, 15 families with a total of 70 people remained in an emergency shelter at the police athletic league as a result of that fire, said the mayor's director of communications. They include families from the burned building as well as families from the buildings on either side. The families from the neighboring homes will be allowed home after the fire-wrecked apartment building is torn down. Authorities classified the fire as suspicious. A mail carrier and another witness reported seeing children burning papers in front of the 4-story building earlier in the day before the three-alarm fire engulfed the wood-frame structure. The fire burned out of control for nearly 3 hours as some 70 Yonkers firefighters responded, their efforts on the dead-end street hindered by a lack of water.
Source: http://www.lohud.com/article/20120131/NEWS/301310070/UPDATE-70-shelter-displaced-by-2-Yonkers-fires-1-burned-building-set-demolition?odyssey=nav|head

53. *January 31, Associated Press* – (Nevada) **Nevada officials: Luxor guests had Legionnaires'.** Health officials in Las Vegas said January 30 the bacteria that causes Legionnaires' disease was found in water samples at the Luxor hotel-casino in January after a guest died of the form of pneumonia. The Southern Nevada Health District said the Centers for Disease Control and Prevention national surveillance program reported three cases in the past year of Luxor guests being diagnosed with the disease caused by Legionella bacteria. The Las Vegas Strip resort's water was tested after the first two cases were reported during the spring of 2011, but no Legionella bacteria was detected, district officials said. Officials said the Luxor, owned by MGM Resorts International, immediately began a remediation process once the bacteria was found. An MGM Resorts spokesman said treatment procedures include superheating and super-chlorination of the water system. The spokesman said the company's resorts regularly test for Legionella and treat water systems preventatively, before bacteria are detected. The new cases come as the company is already facing a civil lawsuit from guests who said they were infected with Legionella at the Aria Resort & Casino, part of the CityCenter complex that is half-owned by MGM Resorts. MGM Resorts notified guests that they might have been exposed to the bacteria between June 21 and July 4, 2011 after the district reported six cases of Legionnaires' disease in July.
Source: http://www.google.com/hostednews/ap/article/ALeqM5ixz-lNAaCBfnEhVp_MZSqge3YVeg?docId=a235210765334c6fb3032a4023d9c788

54. *January 31, ABC News* – (New York) **Shopping cart thrown from above injures 2.** A shopping cart that critically injured two men might have been used as a weapon in a dispute between taxi drivers competing for fares outside a New York City shopping center, according to a taxi driver representative, ABC News reported January 31. The men were hit after the cart plummeted three stories at Mott Haven Mall in the Bronx. The New York City Police Department said it is reviewing surveillance video of the incident to determine what happened. This is the second time in 3 months a shopping cart was pushed from a higher floor and landed on a shopper. A woman went into a coma after two boys pushed a shopping cart from a fourth-four parking garage in New York City October 30.

Source: http://abcnews.go.com/blogs/headlines/2012/01/shopping-cart-thrown-from-above-injures-2/

55. *January 31, Associated Press* – (Virginia) **Vandals caused $60,000 in damage to mosque under construction in Va.** Fairfax County police said vandals did extensive damage to a mosque under construction in Chantilly, Virginia. Police received a report of destruction of property at the Ahmadiyya Muslim Community Mosque January 30. The Washington Post reported the mosque's first-floor windows and glass were shattered by rocks. Damage was estimated at $60,000. Police said there was no sign the building was entered. Several discarded liquor bottles were strewn around the grounds.
Source: http://www.washingtonpost.com/local/vandals-caused-60000-in-damage-to-mosque-under-construction-in-va/2012/01/31/gIQAw7i5fQ_story.html

56. *January 31, Fort Wayne Journal Gazette* – (Indiana) **Bombs found after apartment blast.** Police found several bombs and ingredients to make more explosives inside an apartment in Fort Wayne, Indiana, while the man who lived there remained hospitalized after his hand was blown off in the explosion, the Fort Wayne Journal Gazette reported January 31. Fort Wayne's hazardous devices unit collected several chemicals, fuels, and powders used to make bombs and several bombs from an apartment at the River Cove Apartment complex, a police spokeswoman said. Police responded January 29 after the man made an explosive mixture that became rocklike and he "began to engage" the mixture with a chisel, causing the explosion. The man's hand took the full force of the explosion. The mixture that exploded was not believed to be a massive explosive device. The police spokeswoman said the man will probably face criminal charges because of the bombs found in his home. The man lived in the home with his teenage son and daughter. The daughter also was injured in the explosion, police said.
Source: http://www.journalgazette.net/article/20120131/LOCAL07/301319982

For another story, see item **57**

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

57. *January 31, Omaha World-Herald* – (Iowa; Missouri) **SWI levee breaches to soon be just a memory.** According to the U.S. Army Corps of Engineers, contractors expect to have levee breaches plugged near Hamburg and Percival, Iowa, and the northwest Missouri village of Watson by March 1, the Omaha World-Herald reported January 31. Repairs to breaches that flooded Percival and the Watson area are expected to be substantially complete February 3, a Corps spokesman in Omaha, Nebraska, said. The

breach that sent floodwaters toward Hamburg in June is targeted to be repaired by mid- to late February. Construction started the week of January 23 on a man-made breach created about 3 miles south of Hamburg to drain floodwaters. Work was originally delayed due to problems gaining access from landowners. More than $160 million was appropriated for the Hamburg and Percival levees alone, but Corps officials expected the costs to end up significantly lower. The Watson levee guards two villages northwest of Rockport, Missouri, Interstate 29, a state highway, 275 structures, and farmland.
Source:
http://www.southwestiowanews.com/council_bluffs/news/local_news/article_d10bb110-4c2d-11e1-a634-001871e3ce6c.html

58. *January 31, Associated Press* – (Colorado) **Rocky Mountain National Park considering options for fixing hazardous dam.** Officials at Rocky Mountain National Park in Estes Park, Colorado, are reviewing options to repair the Lily Lake Dam, located at the headwaters of Fish Creek, after it was rated a high-hazard dam by the U.S. Bureau of Reclamation, the Associate Press reported January 31. Park engineers said failure of the dam is not imminent, but a long-term solution is needed. Options include repairing or removing the dam. In the meantime, the dam will be regularly inspected. Park officials said if the dam were to fail, flooding could result in the loss of life and property along Fish Creek.
Source:
http://www.therepublic.com/view/story/a0743ec6a46f4199b89b163f75ef3ec5/CO--Dam-Hazard/

[Return to top]

Department of Homeland Security (DHS)
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