Daily Open Source Infrastructure Report
20 January 2012

Top Stories

- U.S. prosecutors arrested a Chinese computer programmer January 18 on charges that he stole software code valued at nearly $10 million from the Federal Reserve Bank of New York. – *Reuters* (See item **19**)
- A researcher found multiple denial of service vulnerabilities in Rockwell Automation's FactoryTalk supervisory control and data acquisition product, the Industrial Control Systems Cyber Emergency Response Team announced. – *Infosecurity* (See item **45**)

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. *January 19, Huntington Herald-Dispatch* – (West Virginia) **Derailment serves as lesson for special needs registry.** A train derailment in Huntington, West Virginia, January 17 caused damage to tracks at the CSX rail yard, but no injuries or spills were reported. A CSX representative said the incident occurred at about 10:30 p.m. at the

CSX yard behind the Cabell-Huntington Health Department on 7th Avenue. It involved the derailment of 12 train cars carrying coal. The derailment was spotted by those attending a health department meeting discussing the special needs registry the morning of January 18. The registry, a system designed to provide vital personal and medical information to first responders, public health officials and emergency management agencies in the event of an emergency, was unveiled in November.
Source: http://www.herald-dispatch.com/mobile/x226602562/Derailment-serves-as-lesson-for-registry

2. *January 19, KING 5 Seattle* – (Washington) **Over 110,000 homes without power in freezing temps.** Utility companies in Washington were scrambling after power lines knocked down by snow-heavy tree branches knocked out power to more than 100,000 Puget Sound Energy and Tacoma Public Utilities customers January 19. A Puget Sound Energy spokesman said 90,000 customers were without power. Tacoma Public Utilities posted on their Facebook page that 24,000 homes were without power.
Source: http://www.nwcn.com/news/washington/70000-PSE-customers-without-power-137669193.html

3. *January 18, Associated Press* – (U.S. Virgin Islands) **Major oil refinery to close in US Virgin Islands.** One of the world's largest oil refineries in the U.S. Virgin Islands will close next month, the company announced January 18. Industry analysts said the closure is unlikely to have a major effect on the global oil market. Losses at Hovensa, a joint venture of U.S.-based Hess Corp. and Venezuela's state-owned oil company, have totaled $1.3 billion over the past 3 years and were projected to continue due to reduced demand caused by the global economic slowdown, and increased refining capacity in emerging markets. Hovensa was the third largest U.S. refinery before it cuts its capacity of 500,000 barrels by 30 percent last year. It is now the eighth largest, according to the U.S. Energy Information Administration.
Source: http://abcnews.go.com/Business/wireStory/major-oil-refinery-close-us-virgin-islands-15385253#.TxhIpYHLlBk

For another story, see item **45**

[Return to top]

Chemical Industry Sector

4. *January 19, Nashville Tennessean* – (Tennessee) **Gallatin's Hoeganaes plant hit with 11 fire code violations.** Inspectors found 11 fire code violations this month at the Hoeganaes iron-powder manufacturing plant in Gallatin, Tennessee, where five workers were killed in 2011 in three separate fires, the Nashville Tennessean reported January 19. One violation involved a small amount of combustible dust accumulation under a conveyor system. Dust buildup was criticized and implicated in the deadly accidents, and officials with the U.S. Chemical Safety Board have urged better practices for controlling the powder. Other findings included inadequate emergency lighting, a fire extinguisher obscured from view, missing covers on at least two electrical junction boxes, obstructed or not clearly marked exits, and compressed gas

cylinders not secured properly. The inspectors also reported the fire alarm system and some exit doors did not meet fire code standards for industrial facilities. The report said contractors working at the plant must be trained according to Hoeganaes safety standards.
Source: http://www.tennessean.com/article/20120119/NEWS01/301190020/Gallatin-s-Hoeganaes-plant-hit-11-fire-code-violations?odyssey=tab|topnews|text|FRONTPAGE

5. *January 18, Associated Press* – (Louisiana) **La. bulk storage company ordered to pay $350K for discharging toxic chemical into Miss. River.** A Louisiana bulk storage company was ordered to pay $350,000 for illegally discharging a toxic chemical into the Mississippi River. A federal magistrate January 17 ordered Stolthaven New Orleans LLC, of Braithwaite, to pay a $200,000 fine for discharging more than 450,000 gallons of flurosilicic acid from a facility in March 2008. The magistrate also ordered the firm to make $150,000 in "community service" payments to the Louisiana State Police's emergency services unit, the state department of environmental quality, and the Southern Environmental Enforcement Network's enforcement training fund. The firm pleaded guilty in October to violating the Clean Water Act. Prosecutors said the company could have prevented the leak if it had used a rubber-lined tank to properly store the substance.
Source: http://www.therepublic.com/view/story/06a79ecf91ce4b17aaa805c0315e5267/LA--Pollution-Sentence/

For another story, see item **45**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

6. *January 19, London Daily Telegraph* – (International) **Radioactive material stolen from Egyptian nuclear power station.** Radioactive material has been stolen from an under-construction nuclear power station on Egypt's Mediterranean coast that was the site of violent protests, the Egyptian state-run al-Ahram newspaper reported January 19. A safe containing radioactive material at the Dabaa nuclear power plant was seized while another safe containing radioactive material was broken open and part of its contents taken, the newspaper said. The Egyptian government alerted security authorities and asked that specialized teams help in the search for the stolen material. More than a dozen people were wounded the week of January 9 when military police tried to disperse hundreds of protesters demanding the relocation of the plant.
Source: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/9024293/Radioactive-material-stolen-from-Egyptian-nuclear-power-station.html

7. *January 18, Reuters* – (Idaho) **Federal panel faults Idaho lab for radiation exposure mishap.** The radiation exposure of 16 workers at the Idaho National Laboratory in Idaho Falls, Idaho, stemmed from a failure to properly assess the risks posed by the handling of decades-old plutonium fuel cells, federal investigators concluded January

18. In its report on the November 8 mishap, the Department of Energy's Office of Health, Safety, and Security also found the lab erred in not activating its emergency plan sooner after the accident, a delay that may have compromised medical treatment of the workers. Sixteen workers were exposed to low-level plutonium radiation when a container holding a plutonium fuel plate was opened in the process of preparing the material for shipment to another facility. Subsequent inspections found a layer of stainless steel cladding that envelops the spent nuclear fuel inside the container was defective.
Source: http://www.reuters.com/article/2012/01/19/us-nuclear-idaho-idUSTRE80I05W20120119

[Return to top]

Critical Manufacturing Sector

8. *January 19, Deutsche Presse-Agentur* – (International) **Australian safety sleuths blame engine defect for A380 calamity.** An engine oil fire caused by a manufacturing defect in an oil feed pipe almost brought down a Qantas A380 in November 2010, the Australian Transport Safety Bureau said January 19 in its latest update on investigations into the near-disaster. The crippled superjumbo Airbus jet with one of its four Rolls-Royce engines on fire returned to Singapore 15 minutes after take-off and landed without harm to the 466 people aboard. "That defect resulted in fatigue cracking in the pipe, so that oil sprayed into an engine cavity where it ignited because of the high air temperature," the report said, noting the oil fire weakened a turbine disc in the engine. "As a result, the disc separated from its shaft, increased its rotation speed and broke into several parts." Qantas grounded its A380 fleet after the incident, losing millions of dollars in revenue.
Source:
http://www.monstersandcritics.com/news/asiapacific/news/article_1686283.php/Australian-safety-sleuths-blame-engine-defect-for-A380-calamity

9. *January 18, U.S. Department of Labor* – (Wisconsin) **U.S. Department of Labor's OSHA cites Curt Manufacturing in Eau Claire, Wis., after worker's thumb crushed by unguarded machine.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) January 18 cited Curt Manufacturing LLC in Eau Claire, Wisconsin, with eight safety violations, including one willful violation for allowing workers to continue operating an unguarded hydraulic power press brake after a worker was injured. Five serious safety violations were also cited, which involved failing to: develop, document, and use hazardous energy control procedures for machines with multiple energy sources; conduct annual inspections of those procedures; ensure lockout devices were affixed to energy isolating devices by authorized employees; provide point-of-operation guarding on a band saw and tube bender; provide hand tools that permit easy material handling and prevent workers from placing their hands in machine danger zones.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=21663

For more stories, see items **4** and **45**

[Return to top]

Defense Industrial Base Sector

10. *January 18, Aviation Week* – (National) **USAF ranks last in Pentagon testing scorecard.** In the latest annual report from the Pentagon's Director of Operational Test and Evaluation (DOT&E), the U.S. Air Force ranks last among the services in testing performance, with 27 percent of programs reviewed meeting their reliability thresholds, Aviation Week reported January 18. When broken down by service branch, the numbers show the following: 55 percent of the Army programs the office reviewed were able to meet their reliability thresholds, with aviation (CH-47 and UH-72), trucks, and artillery performing well, "while networks and unmanned systems did not do well." Sixty-three percent of the Navy systems studied met reliability thresholds, with the majority of the reliable systems being "aircraft or aircraft-related systems developed in [Naval Air Systems Command]," the DOT&E chief notes. "Other reliable systems were submarines and related systems such as the USS Virginia, USS Ohio, and the TB-34 towed array." The Air Force did not fare well, with only 3 of 11 reviewed programs meeting reliability thresholds. "The three systems that performed reliably were the B-2 Radar Modernization Program, Space Based Surveillance System, and the C-5 Reliability Improvement and Re-Engining Program," the chief writes, while "other programs such as Small Diameter Bomb, Global Broadcast Service, Joint Mission Planning System, MQ-9 Reaper, Miniature Air-Launched Decoy, C-27J Joint Cargo Aircraft, and Global Hawk demonstrated poor reliability." While the report concludes testing and test requirements normally do not cause major delays or drive costs, issues such as quality control, software development, scheduling, and poor performance during testing are factors that have caused program delays.
Source:
http://www.aviationweek.com/aw/generic/story.jsp?id=news/asd/2012/01/18/08.xml&headline=USAF Ranks Last In Pentagon Testing Scorecard&channel=defense

11. *January 18, Defense News* – (National) **Lockheed touts fix for F-35 fuel dump.** According to a top Lockheed Martin official, the company found a way to fix the F-35 Lightning II's fuel dump system, eliminating a potential fire hazard, Defense News reported January 18. "We expect to have that configuration change back in the test airplane early this year," said Lockheed's Joint Strike Fighter program manager. "The permanent modification that will go into all the production airplanes will be tested by the second quarter of [2012]." The current test aircraft fleet has an interim solution installed, he said. In conventional aircraft, fuel can be dumped through a mast that ejects the fluid away from the aircraft's surfaces. But to keep the F-35 stealthy, the design pumped fuel out forcefully from a valve flush with the wing, the program manager said. This design allowed a portion of dumped fuel to move back toward the aircraft's structure. On the Marine Corps' F-35B version of the aircraft in particular, the fuel could flow too close to the roll-post ducts, part of the short-takeoff-and-vertical-landing system, and potentially ignite. The problem came to light in a November 2011 report to the Pentagon's acting procurement czar compiled by the Defense

Department's top operational tester.
Source:
http://www.defensenews.com/article/20120118/DEFREG02/301180006/Lockheed-Touts-Fix-F-35-Fuel-Dump?odyssey=tab|topnews|text|FRONTPAGE

For another story, see item **45**

[Return to top]

Banking and Finance Sector

12. *January 19, Associated Press* – (Connecticut) **Naugatuck man pleads guilty to mortgage fraud scheme over a decade, costing lenders $7 million.** A Naugatuck, Connecticut man has pleaded guilty to charges of participating in a mortgage fraud scheme that lasted a decade and cost lenders $7 million, the Associated Press reported January 19. A U.S. attorney said the man and two New York residents obtained fraudulent mortgages to buy more than 40 multi-family properties in Bridgeport. Authorities said the loan applications contained false information about the buyers' finances and property ownership, and false documents such as letters from fictitious employers, earnings statements, and fraudulent bank records. The man pleaded guilty January 18 in federal court in Hartford to conspiracy to commit wire fraud and conspiracy to commit money laundering. He faces a maximum prison term of 40 years. The two New York residents have pleaded guilty to the same charges and await sentencing.
Source:
http://www.therepublic.com/view/story/b59831244a104c399800d9d7d2fbb97a/CT--Mortgage-Fraud-Plea/

13. *January 18, Help Net Security* – (International) **Bogus Western Union notice leads to phishing.** A fake Western Union notice is hitting inboxes around the world and scaring people into following the offered link to a phishing page, Help Net Security reported January 18. "Failure in updating your profile will result in limiting your account access," the spam e-mail says, signed by an "IT Assistant." Users who fall for the trick are taken to a log-in page mimicking the Western Union one. Once they have entered the log-in credentials and pressed the "Sign In" button, they are asked to share information such as date of birth and answers to typical security questions such as their mother's maiden name or favorite pet's name. According to Hoax-Slayer: "Once they have this information, the scammers can then login to the victim's real Western Union account and use it for nefarious purposes such as money laundering. The scammers may be able to use the stolen 'Test Question' details to collect payments without having the user's proper identification documents." Once the victims have done all that has been asked of them, they are redirected to the legitimate Western Union page.
Source: http://www.net-security.org/secworld.php?id=12237

14. *January 18, Venice Patch* – (California) **'Explosives Threat' Bandit linked to robbery of Venice bank.** The so-called "Explosives Threat" bandit has been linked to a January 17 robbery of a Chase Bank in Venice, California, authorities said January

18. He also hit a bank January 17 in the Palms area, a spokeswoman for the FBI's Los Angeles field office said. The robber, who is wanted for multiple heists in Los Angeles County, got his name because he leaves a device in the bank that requires a bomb squad response to render it safe, she said. In a December 2011 press release, the FBI said the robber stuck up a Bank of America November 15 in West Covina and a Bank of America November 28 in West Hollywood. The suspect has left a device made up of electronic components and wiring during each robbery and stated someone outside the bank would detonate it. The suspect made an oral demand and handed a note to the teller in both robberies and demanded as much as $20,000 in cash, the December release said. The FBI said the suspect's notes indicated he had a friend monitoring a police frequency outside the bank and he would make a call telling his friend to "press a button", and one note said once his friend was contacted the "establishment will not exist," the release said.
Source: http://venice.patch.com/articles/explosives-threat-bandit-linked-to-robbery-of-venice-bank

15. *January 18, Chicago Tribune* – (Illinois) **FBI searches for bank robber dubbed 'Wicker Park Bandit'.** The FBI is asking for help identifying a man dubbed the "Wicker Park Bandit" who officials believe was responsible for at least seven bank robberies on Chicago's north side, the Chicago Tribune reported January 18. In all of the robberies, the man entered the bank and approached a teller with a handwritten demand note, the FBI said. The most recent robbery took place January 16 at a North Community Bank branch, officials said. The same robber was also suspected of hitting two other North Community Bank branches January 9 and January 6, officials said. On December 13, the bandit made off with an undisclosed amount of money from the Chase Bank, then later robbed another Chase branch December 30. On December 22, the bandit traveled to the Uptown neighborhood and robbed a PNC Bank branch, officials said.
Source: http://articles.chicagotribune.com/2012-01-18/news/chi-fbi-searches-for-bank-robber-dubbed-wicker-park-bandit-20120118_1_fbi-searches-wicker-park-bandit-chase-bank

16. *January 18, Huffington Post* – (National) **Municipal securities market lacks oversight, says GAO.** Government oversight of the $3.7 trillion market for municipal securities, wracked by several high-profile cases of fraud and bid-rigging, is inadequate, according to a report by the Government Accountability Office (GAO) released January 17. The securities, used by state and local governments to finance transportation projects and the construction of housing, hospitals, and schools, have been the subject of a 5-year federal investigation into the reinvestment of proceeds of municipal bond sales. The Securities and Exchange Commission (SEC) enforces the rules written by two self-regulatory organizations with oversight of the market — the Municipal Securities Rulemaking Board (MSRB) and the Financial Industry Regulatory Authority (FINRA). But because of huge staff cuts at the SEC inspection arm — from 62 inspectors in 2005 to 38 in 2011 — it has checked neither the MSRB nor FINRA's fixed-income surveillance programs since 2005. The SEC's last inspection "predated the financial crisis — and its ensuing volatility in the municipal market," the report says. Without such oversight, "the SEC may be unable to identify

and act on regulatory problems in a timely manner." The SEC recently began to look at FINRA's program, including municipal trade reporting and markup reviews. It has not begun a fresh review of the MSRB. In addition, the report found the market favors institutional investors over individuals with better information and prices.
Source: http://www.huffingtonpost.com/2012/01/18/municipal-securities-mark_n_1214418.html

17. *January 18, Bloomberg* – (New Jersey) **Ex-Columbus Hill Capital CFO admits embezzling $10.4 million.** The former chief financial officer (CFO) of Columbus Hill Capital Management LP, an investment management firm based in Short Hills, New Jersey, pleaded guilty January 18 to embezzling more than $10.4 million. He admitted in federal court in Newark he created a phony account to collect deposits he stole from the company. The CFO, who pleaded guilty to wire fraud and tax evasion, agreed to forfeit the entire amount he stole. He faces as many as 20 years in prison on the fraud charge, and 5 years on the tax evasion count.
Source: http://www.businessweek.com/news/2012-01-18/ex-columbus-hill-capital-cfo-admits-embezzling-10-4-million.html

18. *January 18, Bloomberg* – (Florida) **TD Bank loses $67 million verdict over Rothstein fraud role.** Toronto-Dominion Bank (TD Bank) January 18 lost a $67 million jury verdict over claims it helped a disbarred Florida attorney who admitted running a $1.2 billion Ponzi scheme, by telling victims their money was safe as he depleted accounts. A jury in federal court in Miami returned the verdict in a lawsuit brought by Coquina Investments, based in Corpus Christi, Texas. Coquina's lawyer January 17 urged the jury to award $32 million in compensatory damages, and $140 million in punitive damages. The January 18 verdict was for $32 million in compensatory damages and $35 million in punitive damages. In its complaint, Coquina said officers of the bank "played an active role in the scheme and facilitated its continued existence" by meeting with victims to create the appearance of a legitimate enterprise. While operating the fraud, the lawyer told his victims they were buying stakes in settlements of cases about which his Fort Lauderdale, Florida law firm, Rothstein Rosenfeldt Adler PA, had amassed evidence and confronted potential defendants in sexual and employment discrimination cases. The settlements were fictional, as were the cases. He used the bank to make payments to investors that supposedly came from settlements, and to provide documents "to conceal the truth from the investors, to keep the investors and encourage them to re-invest, and to attract additional investors," according to the complaint. Investors regularly met with the bank's vice president, contributing to the "aura of legitimacy," Coquina said. The bank is facing three other suits by groups of investors claiming it helped keep the fraud afloat by providing the lawyer with documents he used to convince investors their money was safe and could be disbursed only to him, when he actually was siphoning money out of accounts.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2012/01/18/bloomberg_articlesLY09PI6JTSE801-LY0ED.DTL

19. *January 18, Reuters* – (New York; National) **U.S. charges Chinese man with NY Fed software theft.** U.S. prosecutors arrested a Chinese computer programmer January 18 on charges that he stole software code valued at nearly $10 million from the Federal

Reserve Bank of New York. The man was a contract programmer. He was accused of illegally copying software to an external hard drive, according to a criminal complaint filed in U.S. district court in Manhattan. Authorities said the software, owned by the U.S. Treasury Department, cost about $9.5 million to develop. A New York Fed spokesman said in a statement the bank immediately investigated the breach when it was uncovered and promptly notified authorities. The programmer was charged with one count of stealing U.S. government property, which carries a maximum 10-year prison term. The complaint, signed by an FBI agent, said the man admitted to copying the code onto a drive and taking it home. He told investigators he took the code "for private use and in order to ensure that it was available to him in the event that he lost his job," the complaint said. While U.S. intelligence officials have become increasingly worried about economic espionage, cybercrime experts said the case appeared to be one of simple theft. The programmer was hired as a contract employee in May by an unnamed technology consulting company used by the Fed to work on its computers, the complaint said. The code, called the Government-wide Accounting and Reporting Program (GWA), was developed to track the billions the U.S. government transfers daily. The GWA provides federal agencies with a statement of their account balance, the complaint said. Investigators uncovered the suspected breach only after one of the programmer's colleagues told a supervisor the programmer had claimed to have lost a hard drive containing the code, the complaint said.
Source: http://www.reuters.com/article/2012/01/19/us-nyfed-theft-idUSTRE80H27L20120119

20. *January 17, St. Louis Post-Dispatch* – (Missouri) **SEC alleges Clayton-based Acartha Group CEO committed fraud.** The Securities and Exchange Commission (SEC) has alleged that Clayton, Missouri-based Acartha Group and its owner fraudulently used $9.1 million in investor funds over several years for the owner's personal use. The SEC filed a federal lawsuit in a St. Louis court January 17 detailing its fraud charges against Acartha, its owner, MIC VII LLC, Acartha Technology Partners LP (ATP), and Gryphon Investments III LLC. The owner is the chief executive officer (CEO) and chairman of Acartha Group, a private equity fund management company. MIC VII and ATP are private equity funds, and Gryphon is a general partner of ATP. The CEO and the related investment entities raised $88 million from 97 investors from 2003 until last year, according to the SEC's complaint. However, without the investors' knowledge, the CEO misappropriated more than $9 million for his personal use, including to pay alimony, buy luxury automobiles, lease a private airplane and helicopter, and take expensive vacations, the SEC alleged.
Source: http://www.stltoday.com/business/local/sec-alleges-acartha-group-ceo-committed-fraud/article_0f00cb42-412d-11e1-bfbe-001a4bcf6878.html

[Return to top]

Transportation Sector

21. *January 19, Washington Post* – (District of Columbia; Virginia) **Two Metro employees accused of stealing thousands.** Two Washington Metropolitan Area Transit Authority (Metro) workers have been accused of stealing thousands of dollars

in coins from stations throughout the Washington D.C. region, federal authorities announced January 19. One suspect who worked as a revenue technician, and the other, a transit police officer, were tasked with collecting fares and taking the money to Metro's revenue collection facility in Alexandria, Virginia, authorities said. Beginning in 2010, they stole thousands, sometimes stashing bags of change under an overpass and collecting them after their shifts had ended, authorities alleged in court papers. The officer used stolen money to buy Virginia lottery tickets — sometimes paid for with bags of change. Between October and December, one suspect paid more than $28,000 in cash and coins to buy tickets, states an affidavit filed by a captain with the Metro Transit Police Department. The suspects are charged with conspiring to commit theft from programs receiving federal funds. Both men were arrested January 18 and were scheduled to appear January 19 in federal court in Alexandria.
Source: http://www.washingtonpost.com/blogs/crime-scene/post/two-metro-employees-accused-of-stealing-thousands/2012/01/19/gIQAhDOdAQ_blog.html

22. *January 19, Reuters* – (Mississippi) **Air controller error blamed in U.S. near-miss.** U.S. safety investigators January 18 cited air traffic controller error for a near mid-air collision of a commuter jet and a small plane last year in Mississippi. The National Transportation Safety Board (NTSB) said the ExpressJet flight with 53 people aboard and a single-engine Cessna 172 came within 300 feet of each other over the Gulfport-Biloxi airport June 19. Both took off nearly simultaneously from intersecting runways after receiving clearance to do so from the airport tower staffed by Federal Aviation Administration (FAA) controllers, the NTSB said. The crew of the ExpressJet Embraer 145 operating as a United/Continental flight to Houston did not sense a potential conflict even though the two were monitoring radio traffic and acknowledged the other plane had also been cleared for takeoff from the other runway, NTSB interview transcripts showed. The crew said their plane's automatic proximity warning system did not sound and there was no need to take evasive action. The commuter plane flew on to Houston where it landed later that afternoon. The Cessna was ordered to go around the airport following takeoff to remove it from any danger. The safety board documents alleged the controller in question had a history of "professional deficiencies" that included non-compliance with standard checklist procedures. The FAA said in a statement it made management changes at Gulfport following the incident, and suspended and decertified the controller involved. The controller has since been retrained and is back on the job.
Source: http://www.reuters.com/article/2012/01/19/uk-usa-airlines-nearmiss-idUSLNE80I01S20120119

23. *January 19, Pittsburgh Post-Gazette* – (Pennsylvania) **Panhandle Bridge reopens and T moving after barge wrecks.** The Panhandle Bridge, which carries light-rail traffic over the Monongahela River, in Pittsburgh, reopened after inspectors determined runaway barges that passed underneath it scuffed its piers but caused no structural damage, the Pittsburgh Post-Gazette reported January 19. A spokesman said T train cars were running on the bridge. The bridge was one of four that shut down and reopened after three barges carrying coal broke free early January 19, said a public information officer for the Coast Guard Marine Safety Unit Pittsburgh. The Liberty Bridge, Smithfield Street Bridge, and Fort Pitt Bridge reopened after being inspected.

The Monongahela River remained closed to river traffic. A portion of the Ohio River also remained closed, but traffic can still travel from the Allegheny River to the Ohio River. The spokesman said two barges broke loose from a towboat somewhere on the Monongahela River between 1:30 a.m. and 2:30 a.m. One barge floated into a fleeting area where other barges were moored, causing another barge to break free. Those two floated to the Smithfield Street Bridge, where they stopped and were collected by a towboat. Another barge struck the Fort Pitt Bridge and sank. Inspectors are determining whether the sunk barge is compromising the structure of the bridge. If it is, they will work to remove it.
Source: http://www.post-gazette.com/pg/12019/1204573-100.stm

24. *January 19, CNN* – (Oregon; Washington) **As snow slows, roads get icy in Pacific Northwest.** A day after heavy snowfall made Seattle streets look more like ski runs, freezing rain and accumulating ice shut down runways at the city's airport January 19 and made travel even more treacherous. The National Weather Service issued an ice storm warning for the Seattle-Tacoma metropolitan area, portions of the coastline, and the southwest interior, including the capital, Olympia. Seattle's public schools remained closed January 19. Ice prompted the closure of two of three runways at Seattle-Tacoma International Airport, officials said, but operations were not affected. As the snowfall slowed January 18, officials warned falling temperatures were making roads dangerous. An avalanche warning was issued for Washington's mountainous areas following heavy snowfall in the Cascades. On January 18, melting snow and heavy rain caused flooding problems in southwest Washington and northwest Oregon, authorities said. Floods contributed to a car accident in Albany, Oregon, January 18, said a spokeswoman for the Albany Fire Department. The car full of people drove into deep water and was swept into a canal. Two people were rescued, and a child's body was recovered.
Source: http://www.cnn.com/2012/01/19/us/northwest-winter-storms/?hpt=tr_c2

25. *January 18, Government Computer News* – (National) **TSA adopts Coast Guard's emergency notification system.** The Transportation Security Administration (TSA) will begin using the U.S. Coast Guard's (USCG) enterprisewide emergency mass notification system. Interagency cooperation is allowing TSA to integrate the infrastructure of the USCG Alert and Warning System (AWS). The system is designed to provide emergency alerts over multiple channels such as landlines, mobile and satellite phones, e-mail, text messages, and facsimile to units across the agency, AtHoc company officials said. The emergency notification system is based on AtHoc's IWSAlerts software. The system will reach 50,000 TSA employees nationwide via a virtual private cloud. The notification will contact units at more than 100 ports and 45 airports, across TSA's Transportation Threat Assessment and Credentialing network, and TSA facilities. The system's enterprisewide architecture allows deployment in centralized data centers to support TSA facilities. A unified design methodology provides centralized alert activation, control and management from a Web-based console. The USCG has used AWS since 2007. It uses AWS 2.0 for emergency alerts; staff recall; personnel accountability; and disaster response to events.
Source: http://gcn.com/articles/2012/01/18/tsa-coast-guard-emergency-alert-system.aspx

26. *January 18, KXAS 5 Dallas-Fort Worth* – (Texas) **Woman slips through security at DFW with gun.** A woman was taken into custody at Dallas-Fort Worth International Airport (DFW) in Texas, January 18 after getting through a security checkpoint with a gun. The breach at Terminal D's Gate 30 checkpoint was first reported after a passenger slipped through security with a gun in her bag. According to sources, the gun was detected by Transportation Security Administration (TSA) agents after the woman passed through security and entered the terminal. The TSA said the woman left the checkpoint before the screening was over and without turning the weapon over to authorities. Officials then shut down the terminal while they searched for her. She was found a short time later and questioned. About an hour later, she was brought outside of the terminal and placed into a waiting DFW Airport police car. The woman was a ticketed passenger on American Airlines (AA) flight 2385 to Houston. An AA spokesman said the breach delayed about 10 flights, each about 20-25 minutes.
Source: http://overheadbin.msnbc.msn.com/_news/2012/01/18/10182197-woman-slips-through-security-at-dfw-with-gun

27. *January 18, U.S. Department of Labor* – (Arkansas; Missouri) **U.S. Dept. of Labor's OSHA cites American Railcar Industries for safety violations following electrocution of worker near Maumelle.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) January 18, cited American Railcar Industries Inc., headquartered in Saint Charles, Missouri, for 10 serious safety violations after an employee was electrocuted while performing repair work on a tanker-style railcar July 25 at the company's work site near Marmaduke, Arkansas. Upon receiving the fatality report, the OSHA initiated an investigation at the facility on Highway 34 East and found workers were being exposed to electrical shocks from welding equipment. The violations include failing to: provide personal protection for employees conducting cutting and welding operations; properly mark the power supply and control boxes for voltage, current and wattage; use fixed wiring instead of flexible cords and protect the wiring from possible damage; remove defective electrical equipment from service; inspect and mark web slings. A serious violation occurs when there is substantial probability death or serious physical harm could result from a hazard about which the employer knew or should have known. American Railcar designs and manufactures railcars. Proposed penalties total $61,400.
Source: http://www.todaysthv.com/news/story.aspx?storyid=191131

28. *January 18, WFAA 8 Dallas-Forth Worth* – (Texas) **Dallas police have suspect in DART shooting.** Dallas police took over the investigation of the shooting death of a Dallas Area Rapid Transit (DART) passenger January 18 and department officials said they now have a suspect in custody. Police said their suspect is a 20-year-old man, but he has not yet been charged with the crime. The shooting victim died after he was shot twice in the stomach. Dallas police said they spent the morning interviewing two witnesses who said the shooting began as an argument on the platform at DART's Pearl Station. A DART spokesperson said the operator of the train called 911 to report the shooting just after midnight. Dallas Police and DART police arrived immediately.
Source: http://www.wfaa.com/news/local/Dallas-police-have-suspect-in-DART-shooting-137595813.html

29. *January 17, Orlando Sentinel* – (Florida) **AirTran must pay damages to Orlando pilot.** AirTran Airways has been ordered to pay more than $1 million in back wages and damages to an Orlando, Florida-based pilot after federal investigators concluded the airline inappropriately fired him after he reported numerous mechanical concerns with the company's aircraft. AirTran will also have to reinstate the pilot, who told the U.S. Department of Labor that he was fired after the airline noticed a sudden spike in his mechanical-malfunction reports and decided to investigate. The agency's Occupational Safety and Health Administration (OSHA) said an investigation by its Whistleblower Protection Program determined there was "reasonable cause to believe that the termination was an act of retaliation" by the airline, according to information released January 17.
Source: http://www.sun-sentinel.com/business/os-airtran-fined-firing-whistleblower-20120117,0,5887982.story

For more stories, see items **1**, **8**, and **30**

[Return to top]

Postal and Shipping Sector

30. *January 18, Charlotte Observer* – (North Caroliina) **I-85 wreck kills UPS driver.** A United Parcel Service (UPS) driver was killed January 18 when his tractor-trailer slammed into a bridge guardrail on Interstate 85 in northern Rowan County, North Carolina. The wreck sent a trailer from the truck flipping over the guardrail onto a road below. The trucker's load of cigarettes was scattered across I-85 and McCanless Road, where one of the rig's two trailers landed. The southbound lanes of I-85 were closed for about 6 hours while crews worked to clear the wreckage and make repairs. A spokesperson for UPS said the driver had a clean driving record. The company said it is looking into the possibility the truck blew a front tire. The North Carolina Highway Patrol said the driver apparently lost control of the truck on a bridge near mile marker 77. The man died at the scene.
Source: http://www.charlotteobserver.com/2012/01/18/2936524/traffic-update-i-85-closed-in.html

[Return to top]

Agriculture and Food Sector

31. *January 19, WCAU 10 Philadelphia* – (International) **Cops: Trainer sold more than 100 horses to slaughterhouse.** A Pennsylvania horse trainer is facing felony charges after she allegedly sold as many as 120 horses to buyers for a Canadian slaughterhouse, the Philadelphia Inquirer reported January 19. State police said a well-known horse trainer and former Devon Horse Show competitor promised owners she could find good homes for their horses when they could no longer race, according to the paper. What she really found for these horses was a quick death, police said. They said she was selling the horses she was in charge of finding homes for to contractors for a Canadian slaughterhouse. There, the horses would be butchered and sent overseas to be

sold as food, the Inquirer reported.
Source: http://usnews.msnbc.msn.com/_news/2012/01/19/10190070-cops-trainer-sold-more-than-100-horses-to-slaughterhouse

32. *January 18, Bloomberg* – (Texas) **Texas confirms first case of citrus greening in orange grove.** Texas and federal officials confirmed the state's first case of citrus greening, a plant disease that has caused extensive damage to Florida's orange crop, Bloomberg reported January 18. The disease was found in a tree in a commercial orange grove in San Juan, in Hidalgo County, part of which has been placed under quarantine, the Texas Department of Agriculture said. The case was confirmed by state officials and the U.S. Department of Agriculture's Animal and Plant Health Inspection Service. Texas is the nation's second-biggest producer of grapefruit and the third-largest orange grower with 28,295 acres in commercial production in the Rio Grande Valley. State and federal officials are surveying Hidalgo County to gauge the extent of the disease, which is transmitted by an insect called the citrus psyllid and for which there is no cure, officials said. A revised quarantine zone will be set January 20, based on the findings, it said. The disease affects only the tree and not the fruit, and poses no threat to human health.
Source: http://www.businessweek.com/news/2012-01-18/texas-confirms-first-case-of-citrus-greening-in-orange-grove.html

[Return to top]

Water Sector

33. *January 19, Kewanee Star Courier* – (Illinois) **Three area towns to receive $350,000 infrastructure grantrs.** Three Bureau County communities will each receive $350,000 in federal grant funds for infrastructure improvements, the governor of Illinois said January 18. Receiving the grants are Neponset, for water treatment plant improvements; Sheffield, to install new water mains and replace two failing lift stations; and Wyanet, for sewer system improvements. The governor announced nearly $19 million in federal funding to address the infrastructure needs of 59 small and rural communities. Awarded through the Community Development Assistance Program, the funding will be used to make improvements to water and sewer lines, including replacing water mains, and upgrading stormwater systems.
Source: http://www.starcourier.com/news/x3506992/Three-area-towns-to-receive-350-000-infrastructure-grantrs

34. *January 18, KWES 9 Midland/Odessa* – (Texas) **Water main break leaves thousands in Big Spring without water.** A water main break in Big Spring, Texas, left 3,000 people without water January 18 and forced classes to be canceled in Big Spring and Coahoma. "At approximately 10:30 last [January 17] night, we received a call that we had a main break. We found the leak by the high school parking lot. A 20 inch transmission line is one of our largest transmission lines in the system," the Big Spring assistant city manager said. Officials said cold weather caused the break and 350,000 gallons of water was lost. Water was restored to all customers January 18 around 5:30 p.m.

Source: http://www.newswest9.com/story/16549770/water-main-break-leaves-thousands-in-big-spring-without-water

35. *January 15, KSAT 12 San Antonio* – (Texas) **SAWS station catches fire.** A fire at a San Antonio Water System Station (SAWS) January 15 caused an estimated $100,000 worth of damage, and fire officials said it may take a few weeks to fix. Fire crew driving back from a meeting downtown spotted the smoke coming from the station around noon at the Olmos Basin. Fire officials said the chlorine at the station was not affected and the fire was put out quickly. Although four large electrical panels were damaged in the fire, there was no disruption of water service and the station never shut down because there was another working bank to produce power to run the water, the battalion chief with the San Antonio Fire Department said.
Source: http://www.ksat.com/news/SAWS-station-catches-fire/-/478452/8099324/-/51ung8/-/

36. *January 14, San Francisco Chronicle* – (California) **$1.4 million settlement agreement in sewer spill.** A Menlo Park, California sanitary district agreed to pay $1.4 million to settle a long-running lawsuit accusing the utility of spilling tens of thousands of gallons of sewage into creeks and sloughs that drain into San Francisco Bay, the San Francisco Chronicle reported January 14. The West Bay Sanitary District, which was found liable in May for 21 sewage spills over a 5-year period, will pay the legal fees for San Francisco Baykeeper and use the rest of the money to fund projects that will benefit water quality in the bay, according to the settlement. A federal judge granted summary judgment to Baykeeper in May, approving fines of up to $975,000 in Clean Water Act penalties. A trial was set for March to determine liability for dozens of other spills. Representatives of the sanitary district, which approved the settlement, said major upgrades have already been made and overflows of effluent have been virtually eliminated. Baykeeper accused the district of spilling sewage beginning in 2004 into waterways including San Francisquito Creek, Los Trancos Creek, Bovet Creek, Atherton Channel, Bayfront Canal, Ravenswood Slough, Westpoint Slough, and San Francisco Bay.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/01/13/BAVG1MP8V8.DTL&tsp=1

For more stories, see items **5**, **45**, and **52**

[Return to top]

Public Health and Healthcare Sector

37. *January 18, KSAT 12 San Antonio* – (Texas) **Personal documents found in trash can.** Boxes full of personal medical records were recovered in a Castroville, Texas trash can, exposing thousands of patients' confidential medical records. In addition to medical conditions and treatments, there were names, addresses, phone numbers and social security numbers. KSAT 12 San Antonio traced the records to a company called Ayuda Medical Case Management. The owner said the boxes ended up in a dumpster after he failed to pay the rental on his storage unit and the contents, including the

boxes, were auctioned off.
Source: http://www.ksat.com/news/Personal-documents-found-in-trash-can/-/478452/8282132/-/59y7ox/-/index.html

For another story, see item **49**

[Return to top]

Government Facilities Sector

38. *January 19, Associated Press* – (Kentucky) **Boy, 12, admits starting fire at school.** Authorities in Hebron, Kentucky said a boy started a fire that closed a middle school for a day. A school resource officer extinguished the fire, which was set in a boys' bathroom at Conner Middle School January 18. About 1,200 students and staff were moved to Conner High School across the campus, according to the Kentucky Enquirer. Detectives determined the fire was set intentionally and probably began in a toilet paper dispenser. Police said a sixth-grader admitted starting the fire. Arson charges were pending January 18. Classes were called off about an hour later and students were sent home.
Source: http://www.fox19.com/story/16553166/boy-12-admits-starting-fire-at-school

For more stories, see items **24** and **34**

[Return to top]

Emergency Services Sector

39. *January 19, FireNews.net* – (North Carolina) **NC: No safety breach in Asheville LODD.** A state investigation into the death of an Asheville, North Carolina firefighter during an office building blaze found the city fire department violated no occupational safety rules. But department of labor inspectors also said in findings released January 18 that more could be done to avoid future tragedies. The fire department should improve training to ensure a better system of accounting for personnel during a fire, state investigators said. And the department's rapid intervention team, composed of firefighters whose only job at a blaze is to assist other firefighters who might be in danger, should have more specific assignments and responsibilities along with the equipment needed to handle crises. The firefighter died July 28 while fighting a medical office building fire. Ten other firefighters were injured. He went into cardiac arrest after suffering from exposure to heat and smoke.
Source: http://firenews.net/3080/nc-no-safety-breach-in-asheville-lodd/

40. *January 18, Bangor Daily News* – (Maine) **Police say bomber's motive was revenge for older sister's arrest.** The man being held on $100,000 bail after allegedly planting several homemade explosives at the home of a Waldo County, Maine, Sheriff's Office detective earlier this month had help — and may have been motivated by the detective's arrest of his older sister earlier that day. The suspect also is believed to have placed many more chemical explosive devices in front of the detective's home the

evening of January 4 than the three that had previously been reported, according to a January 18 press release from the sheriff's office. "It was determined that someone had placed a large amount of nails in [the detective's] driveway and had placed nine or ten explosive devices in front of the residence, several of which exploded," the press release stated. The detective was home and heard the explosions, which he reported to the Waldo County Communications Center. Police officials from the Belfast Police Department and the Waldo County Sheriff's Office responded. The suspect was arrested January 5 and charged with criminal use of explosives, aggravated possession of marijuana, and violation of a protection order. Another man was arrested January 13 and charged with criminal use of explosives in connection with the same case. According to the district attorney, the detective had arrested the suspect's 28-year-old sister earlier January 4 on a warrant for outstanding charges.
Source: http://bangordailynews.com/2012/01/18/news/midcoast/police-say-bombers-motive-was-revenge-for-older-sisters-arrest/

41. *January 18, Examiner.com* – (National) **FBI: Nationwide trend of 'swatting' both dangerous and costly.** The FBI has grown increasingly concerned about the number of prank calls to police that warrant mobilizing SWAT teams to respond to hostage situations, which pose a very real threat to citizens and law enforcement officers, Examiner.com reported January 18. On average, each prank call cost $10,000 in resources. The FBI coined the term "swatting" to describe the phenomenon. The latest incident which took place in early January in a Georgia town, demonstrates the serious risks posed to law enforcement officers and communities. Cyber criminals are using modified telephone caller identification that allows them to mask their identities while reporting hostage situations or bomb incidents with the purpose of getting SWAT forces deployed on innocent victims, either for revenge or for bragging rights. Advanced technology allows swatters to appear as though they are calling 911 from the home phone number of their targets while reporting a gruesome murder or a home intrusion. State and local law enforcement agencies around the country are working together with the FBI and telecommunications providers to address swatting incidents.
Source: http://www.examiner.com/homeland-security-in-chicago/fbi-nationwide-trend-of-swatting-both-dangerous-and-costly

42. *January 17, WTSP 10 St. Petersburg* – (Florida) **Cops: Teen threatens to kill officer, blow up police station.** A 16-year-old New Port Richey, Florida, teen is accused of threatening to kill an arresting officer, the officer's family, and blowing up the police station once he is released, WTSP 10 St. Petersburg reported January 17. According to a Pasco County Sheriff's Office report, the 16-year-old was being arrested when he began fighting with officers. The report said he was spitting and banging his head on the patrol car. Officers shackled and hobbled him, but he continued to spit and tried to bite one officer. He was then fitted with a spit mask. He allegedly began screaming for the officer to take off his handcuffs, because he was going to blow up the police station with a bomb. He was taken by officers to Northbay Hospital after he told them he had taken two "Roxy" pills 2 hours prior. Once at the hospital, he continued to threaten the officer's life and told him once he got out of the juvenile detention center he was going to get his "boys" and come to the officer's home to kill him and his family. He also threatened again to blow up the police station. He was charged with disorderly conduct,

resisting arrest with violence, two counts threatening public servant, and threat to discharge a destructive device.
Source: http://www.wtsp.com/news/article/232712/8/Cops-Teen-threatens-to-kill-officer-blow-up-police-station

For another story, see item **25**

[Return to top]

Information Technology Sector

43. *January 19, H Security* – (International) **Koobface C&C goes silent after alleged controllers exposed.** The Koobface network is apparently down, according to Facebook. A Facebook security official told Reuters the company's decision to expose the five men alleged to be behind the malware had an effect within 24 hours: "The thing that we are most excited about is that the botnet is down." On January 18, Facebook decided to publish the names of alleged gang members based on details of research carried out in 2009-2010 by two German researchers. One of the researchers works for Security company Sophos. A Sophos researcher told H Security the command and control servers are not down, they just have not sent out any new commands since 08:40 GMT January 17. "Now they just reply with 404 errors" he said. He did note though the five men identified by the investigation "appear to have been busy deleting their social networking accounts."
Source: http://www.h-online.com/security/news/item/Koobface-C-C-goes-silent-after-alleged-controllers-exposed-1416869.html

44. *January 19, Softpedia* – (International) **Scanned documents from Xerox devices hide Blackhole exploit kits.** The malicious technique where cybercriminals send e-mails pretending to come from a scanner inside an office building has been seen again, targeting e-mail accounts of company staff members. This time, an e-mail bearing the subject "Re: Scan from a Xerox W. Pro #XXXXXXX," informs the recipient a document was sent to her from a Xerox device, Websense informs. Confused users, who may not know an employee named MAMIE that sent the e-mail, might rush to click on the link that allegedly points to five image files. Instead, once clicked, the link redirects the user to a Web site that hosts the malevolent Blackhole exploit kit. Hiding in an iframe, the kit looks for vulnerable software and once it finds it, executes a shellcode that triggers the execution and download of other pieces of malware. More than 3,000 of these messages have been discovered so far, but since this variant of the Blackhole kit is more advanced, allowing cybercriminals to tweak the malware, the number may increase. Blackhole is often rented by users and this latest version offers many improvements, such as administration options for smartphones, and an option for the kit to utilize underground audio and video scanners for malware.
Source: http://news.softpedia.com/news/Scanned-Documents-from-Xerox-Devices-Hide-Blackhole-Exploit-Kits-247417.shtml

45. *January 18, Infosecurity* – (International) **SCADA-logical: DoS vulnerabilities in Rockwell Automation FactoryTalk disclosed.** A researcher uncovered multiple

denial of service (DoS) vulnerabilities in Rockwell Automation's FactoryTalk supervisory control and data acquisition (SCADA) product, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) announced January 17. The vulnerabilities are exploitable by sending specially crafted packets to the server, which can result in a DoS attack, according to an ICS-CERT advisory. According to a company brochure, the FactoryTalk product extends the Rockwell Integrated Architecture by providing an information tier of software applications and services for production and performance management. Integration with the Rockwell Logix control platform, as well as connectivity to third-party and legacy systems enables FactoryTalk to deliver high-fidelity data flow across the enterprise. ICS-CERT said it notified Rockwell about the vulnerabilities, which were disclosed by the researcher without coordination with ICS-CERT or the vendor. As it has in past advisories, ICS-CERT recommends users take the following defensive measures to minimize the risk of exploitation of these vulnerabilities: minimize network exposure for all control system device; locate control system networks and devices behind firewalls and isolate them from the business network; and if remote access is required, employ secure methods, such as virtual private networks.
Source: http://www.infosecurity-magazine.com/view/23317/

46. *January 18, TechEye* – (International) **Oracle database has huge flaw.** Oracle's flagship database software has a major flaw that could create serious outages. The hole was found by InfoWorld hacks. It came about because of a collection of problems within the database. Normally, when bugs result in a database outage, the system can be recovered from backups. However, these flaws create such a problem it will take a long time to fix. Oracle said the problem is real and it is spending considerable time and money to fix it. The company released a fix as part of its Oracle Critical Patch Update for January 2012. While an Unpatched Oracle Database customer is vulnerable to malicious attack, the flaw is a special risk to large customers with interconnected databases. The flaws exist in a mechanism deep in the database engine, one most Oracle database administrators seldom see, called the System Change Number (SCN). This is a number that increments sequentially with every database commit: inserts, updates, and deletes, and it is crucial to normal Oracle database operation. Oracle knew SCN needed to be a massive number, so it used a 48-bit number. It should take a long time for an Oracle database to eclipse that number of transactions and pack a sad. However, the number is worked out to a point in time 24 years ago. The problem is, it is unlikely a database has been running constantly since January 1, 1988, processing 16,384 transactions per second. There are many flaws that can force a database to go over this number and hackers could exploit it.
Source: http://news.techeye.net/security/oracle-database-has-huge-flaw

47. *January 18, CNET News* – (International) **McAfee to plug 'spammer' hole this week.** McAfee plans to release a fix soon for a bug in its SaaS for Total Protection anti-malware service that scammers were using to distribute spam, the company said January 18. The problem came to light after McAfee customers reported in blog posts and forum sites that spammers were using a hole in McAfee's RumorServer relay service to secretly send spam from their machines. The customers said they noticed the problem after their e-mails were blocked by e-mail providers, and their IP addresses

appeared on blacklists. The problem is isolated to the SaaS Total Protection service, according to the director of security research at McAfee Labs. There is no evidence that any customer data has been lost or compromised as a result of the problem, he said. "The patch will be released on January 18 or 19, as soon as we have finished testing," he wrote. "Because this is a managed product, all affected customers will automatically receive the patch when it is released. There are two issues with the software. One vulnerability could allow an attacker to misuse an ActiveX control to execute code on the victim's computer. The second one, which is the issue the customers complained about, allows an attacker to misuse the "open relay" technology in the software.
Source: http://news.cnet.com/8301-1009_3-57361542-83/mcafee-to-plug-spammer-hole-this-week/

For another story, see item **19**

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

48. *January 19, StateCollege.com* – (Pennsylvania) **WTAJ transmitting again after earlier equipment failure.** WTAJ 32 Altoona, Pennsylvania, was transmitting again January 19 at least via local cable systems. The station posted online links to a few programs that viewers may have missed during an outage on the evening of January 18. A technical problem kicked the station off the air January 18, WTAJ reported on its Web site. It referred to the problem as an equipment failure.
Source: http://www.statecollege.com/news/local-news/update-wtaj-transmitting-again-after-earlier-equipment-failure-985021/

For more stories, see items **41** and **43**

[Return to top]

Commercial Facilities Sector

49. *January 18, Vacaville Reporter* – (California) **Cause of blaze in Fairfield still unknown.** Investigators from the Bureau of Alcohol, Tobacco, Firearms, and Explosives were on hand in Fairfield, California, January 17, along with other Solano County fire investigators, as the probe into a five-alarm fire that gutted an office building January 13 continued, authorities reported. A Fairfield fire captain said that although the cause of the fire remains "undetermined" and under investigation, authorities were veering away from arson as a leading factor. The fire resulted in the

response of about 50 firefighters from five departments. Early estimates put the fire's damage in the millions of dollars. Among the offices housed in the building were the American Cancer Society, the Solano County Bar Association, as well as a number of real estate and psychologist offices, authorities said.
Source: http://www.thereporter.com/news/ci_19764865

50. *January 18, KVII 7 Amarillo* – (Texas) **Fire engulfs Amarillo apartments.** Fire officials contained a large fire at an apartment complex that left at least four families displaced in northeast Amarillo, Texas, January 18. The building became fully engulfed by the flames. The Amarillo Fire Department said the fire was able to get into the attic and caused heavy damage throughout the building. The fire was contained to the original building but an adjacent building was evacuated. A second alarm was dispatched to the fire in order to add more firefighters and trucks. The losses are estimated at $150,000. Fire officials determined the fire was started by an outdoor propane cooker that was being used inside.
Source: http://www.connectamarillo.com/news/story.aspx?id=708978#.TxgqnoHcxfU

51. *January 18, WPVI 6 Philadelphia* – (Pennsylvania) **Fire breaks out at Bucks County shrine.** A well-known Bucks County, Pennsylvania, house of worship was damaged by fire January 18. The fire broke out at the National Shrine of Our Lady of Czestochowa in Doylestown. Crews arrived to find heavy fire and thick smoke billowing from a tower, often used for prayer, located adjacent to the main sanctuary. It took firefighters a little more than a half hour to get the fire under control.
Source: http://abclocal.go.com/wpvi/story?section=news/local&id=8510454

52. *January 17, Los Angeles Times* – (California) **Sewage spill closes beach in Venice, Playa del Rey.** Health officials closed a stretch of beach in Venice and Playa del Rey, California, January 17, after a blocked sewer pipeline upstream released more than 11,000 gallons of sewage. Officials said the spill was contained, and there were no signs of sewage making its way from a city park in Inglewood into nearby Centinela Creek. As a precaution, the Los Angeles County Department of Public Health warned swimmers and surfers to stay out of ocean water a quarter of a mile north and south of the Ballona Creek outlet. Advisories were posted along the beach, which was expected to remain closed until January 19.
Source: http://latimesblogs.latimes.com/lanow/2012/01/16000-gallon-sewage-spill-closes-beach-in-venice-playa-del-rey.html

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

53. *January 18, 6 News Lawrence* – (Kansas) **City to increase height of Alvamar Dam.** Work will begin soon on a dam on Lake Alvamar in Lawrence, Kansas, 6 News Lawrence reported January 18. The project will raise the dam about 6 feet in an effort to keep water from overflowing and causing damage to buildings, homes, and roads in the area. There is nothing wrong with the dam's construction. It holds water, but the height must be increased to protect to the developed areas around it. The lake has been drained since 2007, but will be refilled after the improvements are completed. The project is estimated to cost about $1 million. The city will be contributing about $75,000 toward the construction. The project is expected to be complete by the end of the year.
Source: http://6lawrence.com/news/local/city-to-increase-height-of-alvamar-dam/

[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