Daily Open Source Infrastructure Report
19 January 2012

Top Stories

- A January 13 report from the Pentagon's top tester said the U.S. Air Force grounded its F-22 Raptors in 2011 "due to suspected contamination problems" associated with the environmental control system and onboard oxygen generation system. – *Defense News* (See item)
- Symantec Corp said a 2006 breach led to the theft and January 2012 publication of the source code to its flagship Norton security software. The company reversed its previous position that it was not hacked. – *Reuters* (See item)

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 18, Associated Press* – (New York) **High winds in NY cause power outages for 14K.** More than 14,000 utility customers across upstate New York were without electricity after high winds gusting to more than 50 mph knocked down trees and

power lines. National Grid reported the most outages January 18, with 9,400 customers without power. About 1,800 of the outages were reported in Chautauqua County in the state's southwest corner, with another 1,200 each in Lewis and Onondaga counties in central New York. Another 3,400 customers of Rochester Gas & Electric were without power, most of them in the Rochester area where 6,000 were without electricity earlier in the morning.
Source: http://online.wsj.com/article/AP5571f22bff9743bea2eadf1992b8c890.html

2. *January 18, Associated Press* – (Oregon) **Portland, Ore., power outages as snow turns to rain.** Approximately 30,000 Oregon households in the Portland metro area were without power because of power lines knocked down by a winter storm that moved in January 18. The storm brought some snow, but it changed to rain and the snow quickly began melting, leaving a slushy mix on the roads, cars and trees. Portland General Electric said the customers without power were mainly in Gresham, Oregon City and western Portland. The utility was working to restore service.
Source: http://www.wtnh.com/dpps/weather/us_wx_news/portland-ore-power-outages-as-snow-turns-to-rain-nt12-jgr_4043310

3. *January 17, Kitsap Sun* – (Washington) **EPA fines Navy for problem in monitoring underground fuel tanks.** The U.S. Environmental Protection Agency (EPA) fined the U.S. Navy $161,000 for failing to properly monitor pipes and underground fuel storage tanks for leaks at Naval Base Kitsap-Bangor in Washington, the Kitsap Sun reported January 17. The tanks are supposed to be checked every month. The EPA inspects facilities with underground tanks every 3 years. Bangor was checked in March 2010. It has 53 underground tanks on the base for storing diesel, used oil, and gas, ranging from 170 gallons to 45,000 gallons. EPA inspectors found 37 violations, including failure to properly monitor the tanks and pipes for leaks, failure to have the proper leak-detection equipment installed for the pipes, and failure to provide an adequate alarm system to prevent delivery drivers from overfilling the tanks. The Navy had the right equipment at most of the sites, it just did not monitor it. The service corrected the violations and agreed to provide EPA with documentation showing it is in compliance with proper monitoring.
Source: http://www.kitsapsun.com/news/2012/jan/17/epa-fines-navy-for-problem-in-monitoring-fuel/

4. *January 14, Reuters* – (International) **Mexico pipeline oil spill may take month to clean.** Two weeks after a pipeline leak in coastal Mexico sent oil gushing into a river, state oil monopoly Pemex has recovered about two-thirds of the spilled crude, but the full clean-up could take another month. Mexico's environmental protection agency, Profepa, is supervising containment of the 1,500-barrel spill that killed fish, injured wildlife and left greasy slicks in the Coatzacoalcos river. Pemex blamed the December 31 leak in Veracruz state on vandalism. Fuel thieves routinely tap into Mexico's network of pipelines to steal oil and gas for sale on the black market, often causing small spills. The company has contracted 140 workers to clean up the mess, which it said was mostly contained in a lagoon near the affected valve.
Source: http://www.reuters.com/article/2012/01/14/us-mexico-oil-idUSTRE80D0KY20120114

[Return to top]

Chemical Industry Sector

5. *January 18, KTRK 13 Houston* – (Texas) **Portion of Almeda shut down for chemical leak cleanup.** A chemical leaking from a truck January 18 prompted fire officials to shut down a portion of Almeda Road in Houston. Fire officials said that at around 7:45 a.m., a haz-mat crew was called to Akzo Nobel Surface Chemistry on Almeda near Shadow Creek Parkway. The truck, which was loaded with a cleaning fluid, left the plant and had gone under Beltway 8 when the driver noticed the leak. The driver turned around and went back to the plant. As crews worked to clean up the leak, a portion of Almeda Road was closed.
   Source: http://abclocal.go.com/ktrk/story?section=news/local&id=8509398

6. *January 18, WNEP 16 Scranton* – (Pennsylvania) **Truck crash closes I-81 ramp.** A hazardous materials crew was on the scene of a tractor-trailer crash in Lackawanna County, Pennsylvania, late the morning of January 18. The truck carrying phosphoric acid overturned earlier in the morning at the off-ramp of Interstate 81 north at the Scott/Route 524 exit (199). The ramp was closed as was Route 524 in both directions at I-81 to the intersection of Routes 347/250 in Scott Township. A truck must come from New Jersey to empty the acid from the overturned truck before the truck can be moved. Officials said the hazardous materials crew has a small leak in the truck under control. The state department of transportation expected the ramp and road to reopen around 1 p.m.
   Source: http://www.wnep.com/wnep-lacka-truck-crash-closes-i81-ramp-20120118,0,5941867.story

7. *January 17, myCentralJersey.com* – (New Jersey) **Chemist admits to stealing sanofi-aventis secrets.** A former research chemist with global pharmaceutical company sanofi-aventis headquartered in Bridgewater, New Jersey, pleaded guilty January 17 to stealing trade secrets and making them available for sale through a U.S. subsidiary of a Chinese chemical company, authorities said. The 29-year-old Chinese national is a resident of Franklin, New Jersey, who worked for sanofi-aventis. The convict worked as a research scientist at the firm from August 2006 to June 2011, where she directly assisted in the development of many compounds sanofi-aventis viewed as building blocks for future drugs. The compounds were trade secrets and had not been disclosed outside in any manner, including by means of a patent application. While employed at the firm, the convict was a 50 percent partner in Abby Pharmatech Inc., a subsidiary of Chinese chemical products company Xiamon KAK Science and Technology Co. Ltd. Abby also is engaged in the sale and distribution of pharmaceuticals. The convict admitted that between October 2008 and June 2011, she accessed an internal sanofi-aventis database and downloaded data and chemical structures related to many compounds onto her company-issued laptop. She said she then transferred the data to her home computer via e-mail or a USB thumb drive. The convict further admitted she made the stolen compounds available for sale on the Abby Catalog on Abby Pharmatech Web sites, as well as through a well-known online database. The convict's lawyer said she only listed the items for sale but never had the compounds. He said she

did this to make the size of the Abby Catalog, which included legitimate compounds, look bigger. The charge to which the convict pleaded guilty carries a maximum potential penalty of 10 years in prison and a $250,000 fine.
Source:
http://www.mycentraljersey.com/article/20120117/NJNEWS/301170036/Chemist-admits-to-stealing-sanofi-aventis-secrets

For another story, see item **32**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

8. *January 17, Defense News* – (National) **F-35C tailhook design blamed for landing issues.** Lockheed Martin traced the U.S. Navy F-35C Joint Strike Fighter's troubles with catching a carrier's arresting gear wires to the tailhook design, Defense News reported January 17. Efforts to fix the problem are well underway, a top company official said. The rest of the design of the tailhook system, which include the doors and bay that conceal the device and other ancillary hardware, is sound, the Lockheed program manager for the F-35 program said. A preliminary review has already been completed and was done in conjunction with the Naval Air Systems Command and F-35 Joint Program Office. The program manager said the hook system is already being modified in accordance with the new test data. Tests with the newly modified tailhook should start at Lakehurst, New Jersey, in the second quarter of 2012, he said. That will give the F-35 program another set of data to study to make sure the new design works as promised. However, until those tests are done, there is no ironclad guarantee the redesign of the tailhook will work, but the program manager said he is confident the modified design will be successful.
Source: http://www.defensenews.com/article/20120117/DEFREG02/301170010/F-35C-Tailhook-Design-Blamed-Landing-Issues?odyssey=tab|topnews|img|FRONTPAGE

9. *January 13, Defense News* – (National) **DoD tester: Toxins suspected in 2011 Raptor grounding.** A January 13 report from the Pentagon's top tester said the U.S. Air Force grounded its F-22 Raptors in 2011 "due to suspected contamination problems

associated with the aircraft environmental control system and associated onboard oxygen generation system form later April through late September 2011 (sic)." Compiled by the Pentagon's chief operational tester, the review confirms Defense News' July 25, report that toxins entering the cockpit of the Raptor caused more than a dozen incidents that resembled hypoxia. Since the grounding was lifted in September, the Raptor has flown more than 6,000 times. More incidents have occurred, despite Air Force precautions that include installing charcoal-based filters and having pilots wear pulse-oximeters to alert them of problems. A scientific advisory board quick-look study ordered in 2011 by the Air Force secretary should be finalizing its report either in late January or early February. Sources indicate the service investigators have not found any single explanation for the Raptor's woes. The problem cannot be duplicated on the ground, nor do the hypoxia-like incidents occur during any consistent altitude or phase of flight — if in fact the cause happens in the air.
Source: http://www.defensenews.com/article/20120113/DEFREG02/301130007/DoD-Tester-Toxins-Suspected-2011-Raptor-Grounding

10. *January 13, ABC News* – (National) **F-22 Raptor pilots suffer more apparent oxygen problems.** ABC News reported January 13, pilots for the F-22 fighter plane reported several new instances of experiencing "hypoxia-like" symptoms while at the controls the jet, the U.S. Air Force (USAF) said, an apparently rare but potentially deadly oxygen problem that has stumped the military for the last 4 years. From 2008 to 2011, pilots for the jet reported at least 12 incidents of experiencing the "hypoxia-like" symptoms, prompting the full fleet of F-22s to be grounded in May. After an intense, nearly 5-month investigation, the USAF said it could not figure out what could be making the pilots feel the effects of hypoxia and cautiously sent the pilots back into the skies in October. However, the USAF told ABC News the problem persists — in the 6,000 sorties flown since the grounding, pilots reported another eight instances of suffering "hypoxia-like symptoms." In each of the new cases, the pilot followed proper procedures, returned to base and landed "without incident," the USAF said. "The Air Force has not yet identified a root cause or a single mechanical deficiency, but through a range of both engineering and physiological actions we can mitigate the risk; this includes rigorous inspections, enhanced safety procedures, new training on life support systems, improved physiological monitoring, and continued data collection," a USAF spokesperson said in a statement to ABC News.
Source: http://abcnews.go.com/Blotter/22-raptors-suffer-apparent-oxygen-problems/story?id=15357696#.Txbt3IHpjXN

[Return to top]

Banking and Finance Sector

11. *January 18, Associated Press* – (New York) **Bank of New York Mellon in partial settlement of fraud charges tied to currency trades.** Bank of New York Mellon and the Justice Department (DOJ) have reached a partial settlement regarding charges the bank defrauded customers by offering them unfavorable rates on currency transactions. Under the settlement, announced January 17 by the top federal prosecutor in Manhattan, the bank must disclose how it comes up with currency exchange rates for

customers who buy and sell foreign securities or receive foreign dividends. A federal lawsuit filed in October alleged the bank provided customers exchange rates at the outer margins of what banks offer to each other and made money on the difference. Bank of New York Mellon agreed to stop telling customers they were getting "best execution" prices. Federal prosecutors have sought hundreds of millions of dollars in civil penalties against the bank. The DOJ and the bank will continue contesting that part of the lawsuit.
Source: http://www.washingtonpost.com/business/bank-of-new-york-mellon-in-partial-settlement-of-fraud-charges-tied-to-currency-trades/2012/01/18/gIQAn8g87P_story.html

12. *January 18, Associated Press* – (New York; Massachusetts) **7 charged in $61M single-trade stock fraud case.** A hedge fund co-founder, four financial analysts, and a Dell Inc. employee teamed up in a record-setting insider trading scheme that netted more than $61.8 million in illegal profits based on trades of a single stock from 2008 through 2009, authorities said January 18 as they described a network of friends in finance who made the most of their connections with corrupt employees of technology companies. The scheme was described in a criminal complaint in a U.S. district court that charged four of the men with conspiracy to commit securities fraud and securities fraud, among other charges. Three analysts have already pleaded guilty and are cooperating with the government, according to the court papers. The insider trading plot as authorities described it would be noteworthy for its size. A co-founder at former hedge fund group Level Global Investors LP was among three men arrested January 18. He surrendered to the FBI. An analyst at Sigma Capital Management, an affiliate of hedge fund SAC Capital Advisors in Manhattan, was arrested at his New York City home, while a hedge fund portfolio manager, was arrested in Needham, Massachusetts. It was not immediately clear if the fourth man charged in the complaint was in custody. The illegal profits in the case were made after tips were shared among co-conspirators about upcoming earnings announcements regarding Dell and Nvidia Corp., according to court papers.
Source: http://www.foxnews.com/us/2012/01/18/7-charged-in-61m-single-trade-stock-fraud-case-2118666991/

13. *January 18, The Register* – (International) **New stealthy botnet Trojan holds Facebook users hostage.** A new strain of cybercrime trojan is targeting Facebook users by taking over their machines and shaking them down for cash, The Register reported January 18. Carberp, like its predecessors Zeus and SpyEye, infects machines by tricking users into opening PDFs and Excel documents loaded with malicious code, or attacks computers in drive-by downloads. The hidden malware is designed to steal account information and harvest credentials for e-mail and social-networking sites. A new configuration of the Carberp trojan targets Facebook users to ultimately steal e-cash vouchers. Previous malware attacks on Facebook have been designed purely to steal log-in info, so this latest trojan, spotted by security firm Trusteer, can be considered an escalation. The Carberp variant replaces any Facebook page the user navigates to with a fake page notifying the victim their Facebook account is temporarily locked. The page asks the mark for their first name, last name, e-mail, date of birth, password, and a Ukash 20 euro ($25) voucher number to verify their identity

and unlock the account. The use of anti-debugging and rootkit techniques make Carberp trojan difficult to detect, warns security consultancy Context Information Security. Context said: "Carberp is also part of a botnet that can take full control over infected hosts, while its complicated infection mechanisms and extensive functionality make it a prime candidate for more targeted attacks." Context adds Carberp, which creates a backdoor on infected machines, can be controlled from a central administrator control panel, allowing botnet herders to more easily mine stolen data. Trusteer said it has reported the attack to Facebook.
Source: http://www.theregister.co.uk/2012/01/18/carberp_steals_e_cash_facebook/

14. *January 17, WAPT 16 Jackson* – (Mississippi) **Bank evacuated after smoke fills building.** The Trustmark Bank at Metrocenter Mall in Jackson, Mississippi, was evacuated January 17 after smoke filled the building. Firefighters had to tear the roof to get to the source of the smoke. Witnesses said the smoke started in the attic and then spread into the building, forcing everyone outside. The source appeared to be an electrical short, bank officials said. The bank is expected to remain closed until at least January 20.
Source: http://www.wapt.com/r/30234655/detail.html

15. *January 17, Bloomberg* – (International) **Russian father-son team accused of online fraud by U.S.** A Russian father and son from Moscow have been charged by federal prosecutors in New York with taking part in a scheme to gain illegal computer access to U.S. bank accounts through bogus e-commerce Web sites. The pair was named in an indictment unsealed January 17 in federal court that alleges they and others controlled U.S.-registered companies and operated a business that bought and sold securities. The defendants took unauthorized charges on customers' credit cards by buying the numbers illegally or by malware they surreptitiously installed on victims' computers. The father, arrested last March, arrived in New York January 16 following his extradition by Swiss authorities, the Manhattan U.S. attorney's office said. His son remains at large. The pair held out U.S.-registered firms Sofeco LLC, Pintado LLC, and Tallit LLC as legitimate Internet merchants with Web sites that appeared to offer goods and services. They also engaged in a scheme from June 2004 to February 2005 to gain access to accounts of U.S. victims, and attempted to transfer hundreds of thousands of dollars into bank accounts they controlled at JPMorgan Chase & Co. and a company identified as Asia Europe America's Bank, prosecutors said. The defendants, through Rim Investment Management Ltd., maintained an account at Ameritrade Inc. and bought and sold securities in publicly traded companies. The two men are accused of committing securities fraud by buying and selling thousands of shares of companies by trading in the accounts of U.S. victims, prosecutors said. The indictment describes July 2004 meetings between the pair and unidentified others in Cyprus. Unnamed co-conspirators transferred almost $300,000 from the financial services account of a person in the U.S. to a bank account controlled by the pair.
Source: http://www.businessweek.com/news/2012-01-17/russian-father-son-team-accused-of-online-fraud-by-u-s-.html

16. *January 17, Arizona Republic* – (National) **Chandler man Edward Purvis admits huge Ponzi scam.** For more than 6 years, a con man maintained his innocence in a

fraud that bilked millions from churchgoers in Arizona and 12 other states. But January 17, the man pleaded guilty to orchestrating a Ponzi scheme that involved fake gold mines, phony businesses, and a bogus promise to fund Christian causes with investor money. The man, who has served more than 2 years in state prison for bribery and harassment, was on the verge of going to trial on fraud charges when he withdrew his not guilty plea. As part of a deal with state prosecutors, he admitted illegally controlling an enterprise and fraud, which carries a minimum prison term of 42 months. Authorities said hundreds of victims across the country were duped into giving money to a Christian non-profit owned by the defendant called Nakami Chi Group Ministries International. A partner in 2009 turned state's evidence against the defendant and admitted Nakami was a fraud. The pair promised investors they would receive 24 percent annual returns, and that their money would be used to support Christian causes around the globe. Instead, the defendant used their money for personal investments and expenses. In 2008, the men and their wives were ordered by a civil-court judge to pay $11 million to investors. The chief investigator for the Arizona Corporation Commission testified in 2010 that the defendant and his wife were also tied to an international money-laundering operation involving Caribbean, Swiss, Chinese, and Australian corporations. He said the accounts of one company had been used to pay the wife $5,000 a month since it was opened in 2008. Money was also being sent to Vanuatu Project Limited and a company called California Ore Processing, both of which involve a purported gold mine in the South Pacific. One of Nakami's key investment plans involved gold ore the defendant told investors was worth $120 billion, but in reality was worthless.
Source:
http://www.azcentral.com/arizonarepublic/business/articles/2012/01/17/20120117chandler-man-admits-huge-ponzi-scam.html

17. *January 17, WBOC 16 Salisbury* – (Delaware; Pennsylvania) **Police in Del. seeking fraud suspects.** Delaware State Police (DSP) detectives are asking for the public's help in identifying three suspects wanted in connection with a credit card fraud investigation involving more than 100 victims, WBOC 16 Salisbury reported January 17. The investigation began in April after a man contacted DSP Financial Crimes Unit detectives to report someone had made several unauthorized transactions in Philadelphia using his credit card number. Police said that since the initial report was taken, there have been more than 100 victims of the same type of fraud. Detectives have learned the suspects were able to obtain the victim's credit card numbers and then produced new credit cards. The method the suspects used to obtain the stolen number is still under investigation, according to police.
Source: http://www.wboc.com/story/16536378/police-in-del-seeking-fraud-suspects

18. *January 17, Newark Star-Ledger* – (National) **Newark-based Prudential reaches settlement over death benefits.** Prudential Financial has agreed to improve its practices for identifying deceased life insurance policyholders and pay beneficiaries as part of a settlement reached January 13 with 20 state governments. The life insurer said in a Securities and Exchange Commission (SEC) filing January 13 that it increased its death benefit reserves by $139 million to make payments on potential claims. The settlement, announced by Massachusetts and California officials, was the result of a

2008 probe into 21 insurance companies' compliance with state laws on unclaimed property. State governments were concerned insurance firms sometimes failed to pay death benefits in a timely manner or pay them at all if beneficiaries were not aware of the policies' existence. As part of the settlement, Prudential will review life insurance policies and contracts that were active between 1992 and 2010 using an expanded set of criteria for identifying deceased policyholders and finding their beneficiaries. The criteria includes searching for beneficiaries whose identifying information may be incorrect or incomplete, such as transposed Social Security numbers or misspelled names, a Prudential spokesman said. The settlement could pay up to $20 million to the families of deceased California policyholders alone, the California controller said. So far more than 1,000 Prudential policies, with an average value of $2,000, have been found for individuals in California who have been dead for more than 15 years, he said.
Source:
http://www.nj.com/business/index.ssf/2012/01/prudential_to_revamp_policies.html

19. *January 17, Reuters* – (National) **UBS unit pays $300,000 to settle SEC charges.** An investment advisory arm of Swiss bank UBS will pay $300,000 to settle charges it misled investors by incorrectly pricing certain securities in three of its mutual funds, the Securities and Exchange Commission (SEC) said January 17. The SEC's administrative action against UBS Global Asset Management came on the heels of a referral from SEC examiners who were conducting a routine inspection of the firm. The SEC alleged UBS's failure to properly price securities resulted in a misstatement to investors of the net asset values of those funds. The SEC also claimed UBS did not follow the mutual funds' fair valuation procedures in pricing certain fixed-income securities. In 2008, the UBS unit purchased around $22 million worth of fixed-income securities, most of which were risky mortgage-backed securities not guaranteed by Fannie Mae or Freddie Mac, according to the SEC's order. UBS then valued most of the securities "substantially" higher than what it paid — 100 percent higher in some cases, the government said. The unit had relied on pricing data from third-parties rather than the purchase prices, a violation of the funds' own valuation procedures, the SEC said. UBS did not correct the mistake until more than 2 weeks later, which led the funds' values to be off during part of that time period between 1 cent and 10 cents per share, according to the government.
Source: http://www.reuters.com/article/2012/01/17/us-ubs-settlement-idUSTRE80G1W920120117

20. *January 16, WMAZ 13 Macon* – (National) **Man accused of over $1.5 million financial fraud in Baldwin jail.** A man facing dozens of financial fraud charges in five states has been booked in to the Baldwin County, Georgia jail, WMAZ 13 Macon reported January 16. A Baldwin County Sheriff's Office captain said the man faces financial card transaction fraud and theft charges after the debit card information of a person living in Baldwin County was stolen and used in the Atlanta area. The captain said photos at the bank where the fraudulent transaction was made identified the suspect. He also faces 60 similar counts in Cobb county and 30 in Cherokee, the captain said. He said the suspect is also accused of about $1.5 million in credit card fraud in California.

Source: http://www.13wmaz.com/news/article/162274/153/Man-Accused-of-Over-15-Million-Financial-Fraud-in-Baldwin-Jail

[Return to top]

Transportation Sector

21. *January 18, Associated Press* – (Oregon; Washington) **Washington snow storm: Seattle, Portland cancel flights.** A winter storm blasted the Pacific Northwest January 18, dumping near-record snow in some areas, hammering parts of Oregon with winds as high as 110 mph, and bringing much of the region to a standstill. From the Washington state capital in Olympia to the Oregon coast, schools were closed, roads were clogged with snow and hundreds of accidents, and dozens of flights were cancelled. In an 8-hour period near the capital, there were 95 accidents, a state trooper said. Alaska Airlines announced late January 17 it canceled 38 flights into and out of Seattle and Portland, Oregon. Many court and government offices and libraries closed.
Source: http://www.huffingtonpost.com/2012/01/18/washington-snow-storm_n_1212607.html

22. *January 18, Associated Press* – (California) **Fiery big-rig crash closes interstate for hours.** A fiery freeway crash involving a big-rig and two cars shut down a southern California interstate for nearly 7 hours. The San Bernardino County crash closed both sides of Interstate 10 in Montclair, which is 30 miles east of Los Angeles, late January 17. The cleanup turned the morning commute January 18 into a nightmare with traffic backed up for miles. KNX 1070 Los Angeles said eastbound traffic began rolling at 5:45 a.m., and the California Highway Patrol reopened westbound lanes at 6:20 a.m. Investigators said the big-rig hauling food items got tangled up with two cars in the westbound lanes and slammed into the center divider before bursting into flames. Two people pried out of one of the cars were airlifted to a hospital with non-life threatening injuries.
Source: http://www.mercurynews.com/breaking-news/ci_19765561

23. *January 18, Associated Press* – (Montana) **Freight train from Chicago hits semi in Montana.** A freight train with its whistle blowing derailed January 17 in northeastern Montana after colliding with a semitrailer that had pulled across tracks at a private crossing between Bainville and Culbertson, a BNSF Railway spokesman said. The train traveling from Chicago to Seattle was traveling about 69 mph and had activated its emergency brake, but it struck the semi slightly behind the cab January 17, about 150 feet from U.S. 2, a BNSF spokesman said. The semi was heading from a farm area to the highway. Ten of the train's 40 cars derailed along with four locomotives, including two that were on their sides. The spokesman said about 500 gallons of diesel fuel spilled, but the spill was contained and did not threaten waterways. The cars were carrying everything from plastics to frozen meats, diapers, and washers, some of which spilled. The train also carried small amounts of classified hazardous material, including lighters, adhesives, and alcohol, but there were no environmental threats, the spokesman said. At least 13 trains were rerouted while the track was repaired. Crews were working through the night to repair the track, which could reopen as early as

January 18. About 40 trains typically use the track each day.
Source: http://abclocal.go.com/wls/story?section=news/local&id=8509664

24. *January 17, Associated Press* – (Colorado) **Copper thefts cause $250k in damage to rail system.** Two Colorado brothers are accused of stealing more than $96,000 worth of overhead copper wiring from two light rail construction sites. The Denver Post reported January 17 the thefts caused $250,000 damage to the RTD FasTracks system under construction in Jefferson County, Colorado. Two suspects were being held in Jefferson County jail. One faced charges of theft by receiving, and his brother faced felony charges of criminal mischief and theft. Investigators said about 7,000 feet of copper wire was stolen from one RTD site and another 150 feet from a second, causing I-beams supporting the overhead wires to bend.
Source: http://www.noco5.com/story/16540529/copper-thefts-cause-250k-in-damage-to-rail-system

25. *January 17, Associated Press* – (Texas) **Texas school bus crash sends 32 to hospital.** A tractor-trailer clipped a school bus full of students January 17, flipping the bus onto its side and sending 32 people — 29 of them children — to a central Texas hospital. Police said a 9-year-old boy was ejected through the escape hatch in the bus roof, and the bus driver was knocked unconscious. The accident occurred on Farm-to-Market Road 93 outside Temple, Texas, about 60 miles northeast of Austin. A trooper with the Texas Department of Public Safety said a hardware truck apparently ran a stop sign when it hit the Academy school district bus. Conditions were foggy, but it was unclear whether that factored into the crash, he said. Three of the children being treated were admitted to the hospital, one in critical condition, while the other 26 were discharged, said a spokeswoman for the Scott & White Memorial Hospital. The bus driver also was listed in critical condition, but the other adults, including the truck driver, were treated and discharged. The bus was carrying about 38 children from all grade levels and was on its way to drop students off at the first of three school locations when the crash happened.
Source: http://www.huffingtonpost.com/2012/01/17/texas-school-bus-crash-se_0_n_1211907.html

26. *January 16, WALA 10 Mobile* – (Alabama; Mississippi) **Three arrested in 'big rig' theft ring.** Washington County, Alabama deputies said the wife of one of the suspects in a "big rig" theft ring is now in custody, and they have a strong lead on another suspect. So far, three people have been arrested. Deputies said they are considering two as conspirators. Deputies found a large dump trailer in the back yard of a Washington County house. The owner of the property said his friend dropped it off a month ago. The friend was arrested in connection to several big rig and equipment thefts. The trailer was a key piece to the crime. Investigators noticed the data plate on the trailer was scratched off. A deputy said they found it inside the suspect's house, and discovered it was part of a case of a stolen truck and trailer from Laurel, Mississippi. Deputies said they also found guns, drugs, and more evidence they said could tie the suspect to thefts across at least five states. The suspect's wife was arrested and charged with being a felon in possession of a firearm, possession of drug paraphernalia, and conspiracy to possess stolen property. According to authorities, the man deputies said is

the prime suspect, his wife, and two others who were arrested with the prime suspect as they tried to get away with a stolen 18-wheeler are all in custody. The deputy said as they continue to investigate they anticipate more stolen property to be discovered and also more arrests. Investigators have five large pieces of equipment and trucks but are looking at more. Since the crimes cross state lines the FBI is also investigating.
Source: http://www.fox10tv.com/dpp/news/local_news/three-arrested-in-big-rig-theft-ring

For more stories, see items **5**, **6**, and **60**

[Return to top]

Postal and Shipping Sector

27. *January 17, Scranton Times-Tribune* – (Pennsylvania) **Police say man raided post office in pursuit of bath salt delivery.** A man broke into a closed Clarks Summit, Pennsylvania post office January 16 looking for a package of designer drugs he thought would be there waiting for him, police said. Instead, the man made off with a U.S. Postal Service (USPS) hat and jacket, pieces of mail, a scale, and a coin-operated machine after he could not find the bath salts, even though a tracking of the package indicated it would be at the branch, police said. The man was charged with felony counts of burglary, theft, receiving stolen property, and a misdemeanor count of criminal trespass, after he was spotted driving erratically in a pickup truck. Police found in the truck several opened pieces of mail and the USPS jacket beside him on the front seat, arrest papers said. The man was arraigned January 16 and placed in the county prison in lieu of $35,000 straight bail.
Source: http://thetimes-tribune.com/police-say-man-raided-post-office-in-pursuit-of-bath-salt-delivery-1.1258376#axzz1jiMMNoq2

[Return to top]

Agriculture and Food Sector

28. *January 18, Food Safety News* – (Washington) **Washington state dairy recalls raw milk.** Frisia Dairy and Creamery of Tenino, Washington, is recalling its raw milk because it may be contaminated with a dangerous strain of E. coli, according to a January 17 news release issued by the Washington State Department of Agriculture (WSDA) at the dairy's request. The recall, which covers all expiration dates, was voluntarily initiated by the dairy after the department's routine monthly sampling discovered toxin-producing E. coli in a skim milk sample. The unpasteurized fluid milk products, including whole, skim, and cream, were distributed through on-farm sales and at eight retail outlets in Lewis, Thurston, and Pierce counties. Frisia and the department are continuing their investigation into the source of the problem. The department's news release said E. coli was not found in other samples collected at the same time, nor was it found in previous routine monthly samples.
Source: http://www.foodsafetynews.com/2012/01/washington-state-dairy-recalls-raw-milk/

29. *January 18, Seattle Fire Department* – (Washington) **$300,000 in damages at Belltown apartment complex fire.** Seattle firefighters knocked down a restaurant fire at a Belltown apartment complex that caused a partial evacuation of the 18-story building January 15. A 911 call came in reporting light smoke on several floors of a residential building. Engine Company 2 and 25 battled the heavy flames and intense heat of the first floor restaurant. It took firefighters 15 minutes to knock down the fire. The smoke for the kitchen rose through the ventilation system causing the building's alarm to sound. Several dozen residents self-evacuated. A bus was brought in to provide a warm shelter for the residents who were kept out of their units for about 90 minutes. Seattle fire investigators determined the cause of the fire was electrical originating at an electrical outlet. The damage estimates are $150,000 to the structure and $150,000 to the contents.
Source: http://fdnntv.com/300K-Damages-Belltown-Apartment-Complex-Fire

30. *January 18, Food Safety News* – (National) **Allergen alert: Soy in sunflower seeds.** Ryt-way Industries is recalling select sunflower seeds because they may contain soy ingredients that were not declared on the packaging, Food Safety News reported January 18. The recall is of BIGS Dill Pickle Sunflower Seeds. The sunflower seeds were distributed nationwide in supermarkets, convenience stores, and U.S. military commissaries.
Source: http://www.foodsafetynews.com/2012/01/allergen-alert-soy-in-sunflower-seeds/

31. *January 18, Food Safety News* – (National) **More cakes recalled due to plastic fragment concern.** Price Chopper Supermarkets is recalling two sizes of its bakery's Central Market Classics Tres Leches cakes — the 5 inch and the 8 inch, Food Safety News reported January 18. Rich Foods, the manufacturer of the sponge cake layers contained in these cakes, notified Price Chopper they may contain plastic fragments. Rich Foods recalled the cake about 2 weeks ago, saying small plastic fragments were shredding from defective packaging.
Source: http://www.foodsafetynews.com/2012/01/more-cake-recalled-due-to-plastic-fragment-concern/

32. *January 18, WIVB 4 Buffalo* – (New York) **Fire, HAZMAT crews battle chemical leak.** Firefighters and hazardous materials crews in Buffalo, New York, spent more than 4 hours, from January 17 into January 18, dealing with a chlorine leak in the city's industrial district. Crews were on the scene at ADM Milling. First responders got the company's 18 employees out, put them on a bus, and brought them to a safe area about a half mile away where medics were waiting. One person was taken from the scene by ambulance. The Buffalo fire commissioner said crews made several attempts to stop the leak with the emergency shut-off system, which did not work. Firefighters had to turn off the tanks manually.
Source: http://www.wivb.com/dpp/news/local/chlorine-leak-sends-crews-to-ganson-st

33. *January 18, Associated Press* – (National) **USDA announces $308 million in aid to states.** The nation's top agriculture official announced January 18 that more than $300 million in emergency assistance was awarded to 33 states and Puerto Rico to help them

recover from an unusually intense year for natural disasters across the United States. Utah and Missouri will receive the most disaster aid, together taking in $109 million, or more than one-third of the $308 million in aid from Department of Agriculture (USDA) watershed and conservation emergency funds, the USDA Secretary said. Flooding last spring in Utah inundated thousands of acres of farmland, costing farmers tens of millions of dollars lost to damaged and destroyed crops or delayed planting. Utah will receive $60 million in watershed money for repair work and preventative measures, said the state conservation engineer for the U.S. Natural Resources Conservation Service. Missouri suffered months of flooding along the Missouri River after the U.S. Army Corps of Engineers authorized unprecedented releases from reservoirs in the northern river basin all summer to deal with unexpectedly heavy rain in May and above-average mountain snow-pack. Missouri will receive around $49 million, of which $35 million will come from the watershed program, and the rest from the Farm Service Agency's Emergency Conservation Program.
Source: http://online.wsj.com/article/AP78a8805aa36b40eab19b4d873702b121.html

[Return to top]

Water Sector

34. *January 17, Muncie Star-Press* – (Indiana) **Water-boil advisory extended to today for Selma.** Indiana American Water Co.'s Muncie district extended a precautionary boil-water advisory January 17 for about 1,000 customers on the east side of Muncie, Indiana, and in the Selma area to conduct additional water testing after a 20-inch water main break near Elm and Seymour streets in Muncie January 16. The affected area is generally located east of Gray Street and includes the town of Selma. The main break significantly reduced pressure for customers in the affected area and service was restored around noon after crews were able to isolate the broken section of main. Customers in the affected area were advised to drink and cook with tap water only after boiling it for 5 minutes.
Source: http://www.thestarpress.com/article/20120118/NEWS01/201180311/Water-boil-advisory-extended-today-Selma

[Return to top]

Public Health and Healthcare Sector

See item 7

[Return to top]

Government Facilities Sector

35. *January 18, Fox News; Associated Press* – (District of Columbia) **'Occupy' protesters suspected of throwing smoke bomb over White House fence.** An apparent smoke bomb was thrown over the fence of the White House in Washington, D.C., as hundreds of Occupy protesters massed outside the gates. The crowds were dispersed January 17,

and the White House was all clear. A U.S. Secret Service spokesman said there were no arrests. The U.S. President and First Lady were not home at the time of the incident. The scene outside the White House followed an earlier protest on the West Lawn of the Capitol, in which several hundred protesters affiliated with the Occupy Wall Street movement decried the influence of corporate money in politics and voiced myriad other grievances. Organizers touted the rally, known as Occupy Congress, as the largest national gathering of Occupy protesters to date, and secured a permit that would have allowed up to 10,000 people to participate. While the rally was mostly peaceful, there were some scuffles between police and protesters. U.S. Capitol Police said four people were arrested, one for allegedly assaulting a police officer, and three accused of crossing a police line.
Source: http://www.foxnews.com/politics/2012/01/17/occupy-protesters-suspected-throwing-smoke-bomb-over-white-house-fence/?test=latestnews

36. *January 18, Associated Press* – (California) **San Diego school reopens after arson fire.** A San Diego elementary school reopened January 18, 2 days after an arson that caused $600,000 in damage. The fire January 16 at Alice Birney school damaged the cafeteria, kitchen, and auditorium. It took 50 firefighters 20 minutes to douse the flames. Investigators determined a flammable liquid was used to set the fire. The federal Bureau of Alcohol, Tobacco, Firearms, and Explosives is offering a $5,000 reward for information leading to an arrest.
Source: http://www.mercurynews.com/breaking-news/ci_19765805

37. *January 18, Associated Press* – (North Carolina) **Western NC community college campuses being cleared.** One campus of a western North Carolina community college was secure and another was cleared after a staff member reported seeing a man walking through a parking lot with a handgun, the Associated Press reported January 18. About 1,000 students are on the east campus of Catawba Valley Community College in Hickory. That campus was secure, and police were clearing the main campus, where about 5,000 students attend classes. The Web site of Catawba Valley Community College in Hickory said both campuses were closed and all classes were canceled for the afternoon and evening of January 18. The school president told the Hickory Daily Record it is possible to get from east campus, where the gunman was reported, to the main campus via trails in the woods. Authorities describe the suspect as a white man in his mid-30s.
Source: http://www.wwaytv3.com/2012/01/18/western-nc-community-college-campuses-being-cleared

38. *January 17, CNN* – (District of Columbia) **Man accused of shooting at White House charged in 17-count indictment.** An Idaho man accused of firing a rifle at the White House faces 17 charges, including attempting to assassinate the U.S. President, after being formally indicted by a grand jury in Washington, D.C. January 17. The indictment against the suspect includes new charges such as assaulting officers of the U.S. government with a deadly weapon, injury to U.S. property, namely the White House, use of a firearm during a crime of violence, and assault with a dangerous weapon. The man allegedly fired a rifle at the White House November 11 and then fled. The indictment says the suspect “did forcibly assault, intimidate, and interfere” with

three Secret Service employees by firing at the White House. Several rounds hit the exterior of the White House near the second story residence area for the first family. The suspect was arrested 5 days later in Pennsylvania, and has been jailed ever since.
Source: http://www.cnn.com/2012/01/17/justice/white-house-shooting/index.html

39. *January 13, KOIN 6 Portland* – (Oregon) **Small explosion at David Douglas HS sends 12 to hospital.** Eleven students and a teacher were taken to area hospitals following a small explosion in a science classroom of David Douglas High School in Portland, Oregon, January 13. According to Portland Fire & Rescue (PF&R), a teacher was working with in a sink with a sodium-based metal that suddenly ignited when it came in contact with water. The incident was followed by the release of gas, filling the classroom with smoke. The explosion prompted PF&R to issue a Level 2 hazmat response. Eleven of the 25 students who were in the classroom, along with the teacher, were treated at the scene, most for "upper respiratory distress." The clothing of all 11 students tested for high concentrations of pH, PF&R reported. The communications director for the David Douglas School District said 12 classrooms in the science wing were evacuated, but the rest of the school remained open.
Source: http://www.koinlocal6.com/news/local/story/Small-explosion-at-David-Douglas-HS-sends-12-to/6xOTYAey4keFfu1vobGs8A.cspx

For more stories, see items **3**, **9**, **21**, **30**, **41**, and **55**

[Return to top]

Emergency Services Sector

40. *January 17, New Haven Register* – (Connecticut) **Police: Man impersonating cops used stolen credit card in Old Saybrook, led officers on chase.** After a brief foot chase January 16 in Old Saybrook, Connecticut, local police captured a man who was impersonating police. Police were investigating an incident at a CVS Pharmacy in which a man walked in the store and flashed a police badge and identification while using a stolen credit card to make a purchase. Later, the man was spotted at the Saybrook Point Inn, where he used a gift card he purchased with the stolen credit card to pay for a spa treatment. When police arrived, the man ran off and led them on a foot chase through the first floor and basement of the inn before he was captured.
Source: http://www.shorelinetimes.com/articles/2012/01/17/news/doc4f157b268aff0785055561.txt

41. *January 17, Los Angeles Times* – (California) **LAPD seeks gunman who fired at officers in south L.A.** Police searched January 17 for a gunman who shot at officers from a vehicle in south Los Angeles. No officers were hurt in the incident said a Los Angeles police spokesman. A man in a burgundy-colored car drove up to where a task force of Los Angeles Police Department narcotics detectives and an FBI agent were meeting, got out of his car and opened fire, police said. The man ran from the scene. It was not immediately clear if the man was struck by return gunfire, and police did not say how many shots were fired. Nearby 52nd Street Elementary School was placed on a

lockdown as police swarmed the area and searched for the suspect, police said.
Source: http://latimesblogs.latimes.com/lanow/2012/01/gunman-lapd.html

42. *January 13, WRTV 6 Indianapolis* – (Indiana) **Police gear taken from undercover officer's car.** Police are looking for suspects in the theft of several items from an undercover Indianapolis police officer's vehicle. The thefts happened January 12. The officer said he had stopped at a coffee shop and parked the undercover police car next to the building, WRTV 6 Indianapolis reported. The officer was inside for just a few minutes and found the back window of the car broken when he returned, police said. The officer's .40-caliber police-issued handgun and three loaded magazines were taken, along with his personal 9mm Taurus handgun, a protective vest, handcuffs, two badges, and other equipment.
Source: http://www.theindychannel.com/news/30206156/detail.html

For another story, see item **38**

[Return to top]

Information Technology Sector

43. *January 18, H Security* – (International) **Oracle updates close 78 holes.** Oracle released 78 security patches in its January Critical Patch Updates. The company said these patch day updates address vulnerabilities in "hundreds of Oracle products." Sixteen of the vulnerabilities patched are remotely exploitable without authentication. Affected products include Oracle Database 10g and 11g, Fusion Middleware 11g, Application Server 10g, Outside In Technology, WebLogic Server, versions 11i and 12 of its E-Business Suite, Oracle Transportation Management, JD Edwards, Sun Ray, VM Virtualbox, Virtual Desktop Infrastructure, MySQL Server, and PeopleSoft Enterprise CRM, HCM, and PeopleTools. A vulnerability in Solaris 9, 10, and 11 Express's TCP/IP is the highest rated of these with a CVSS score of 7.8 out of 10.0. The company advises users to install the patches as soon as they become available, because of "the threat posed by a successful attack." Executive summaries of the vulnerabilities can be found in the security advisory.
Source: http://www.h-online.com/security/news/item/Oracle-updates-close-78-holes-1414741.html

44. *January 18, IDG News Service* – (International) **Secunia sets six-month deadline for vulnerability disclosures.** Vulnerability research firm Secunia announced, effective from the beginning of 2012, software vendors will have a 6-month deadline to fix vulnerabilities reported through its Vulnerability Coordination Reward Program. Secunia's previous deadline established in 2003 was 1 year. The decision to reduce it came after studying the history of the company's vulnerability coordination efforts.
Source:
http://www.computerworld.com/s/article/9223513/Secunia_sets_six_month_deadline_for_vulnerability_disclosures?taxonomyId=17

45. *January 18, Help Net Security* – (International) **Facebook 'free mobile recharge' scam hijacks accounts.** A phishing and survey scam rolled into one is currently targeting Facebook users and ends up hijacking their accounts and makes it difficult for users to get them back, warns a McAfee researcher. The victims are lured with messages seemingly posted by friends claiming they received a "100rs free recharge." Following the offered link, users connect to a page asking them to enter Facebook log-in credentials to receive it. Once the account details are entered and the "Log In" button is pressed, the page redirects users to a page mimicking a Facebook one, which asks the user to complete a survey to unlock the recharge option. In the background, the page sends the recorded log-in credentials — in clear text via a HTTP POST request — to a remote server operated by the scammers. The scammers then use the credentials to access the victims' Facebook accounts, change information contained in them (including the password and the e-mail address), and post the same message that lured in the victims in the first place. The affected users are unable to immediately do anything about it. "Even if the victims try to reset their passwords, they will never get the password reset email from Facebook," said the researcher.
Source: http://www.net-security.org/secworld.php?id=12234

46. *January 17, CNET News* – (International) **McAfee software lets scammers hijack PCs to send spam.** McAfee is looking into a problem with a service in its SaaS Endpoint Protection software that appears to be allowing computers to serve as open proxies for sending spam, the company told CNET January 17. "We are aware of the issue and have both threat analytics and development teams diligently analyzing the problem and possible solutions," the company said in a statement. "We will have more information on the issue shortly. "The problem was reported by McAfee customers on the Web who complained their e-mails were being blocked by e-mail providers and their IP addresses were being blacklisted for sending spam. The problem appears to be in the RumorServer Service myAgtSvc.exe, McAfee Peer Distribution Service, which is part of McAfee SaaS Endpoint Protection Suite, previously known as Total Protection Service, according to the Kaamar Blog. The technology, used for delivering updates to computers without a direct Internet connection, serves as an Open Proxy on Port 6515, which effectively opens the computer up to being used to send spam to other sites that looks like it is coming from that IP address, the blog post said.
Source: http://news.cnet.com/8301-1009_3-57360694-83/mcafee-software-lets-scammers-hijack-pcs-to-send-spam/

47. *January 17, Reuters* – (International) **Symantec says hackers stole source code in 2006.** Symantec Corp said a 2006 breach led to the theft of the source code to its flagship Norton security software, reversing its previous position that it had not been hacked. The world's biggest maker of security software previously said hackers stole the code from a third party, but corrected that statement January 17 after an investigation found Symantec's own networks were infiltrated. The unknown hackers obtained the source code to Norton Antivirus Corporate Edition, Norton Internet Security, Norton Utilities, Norton GoBack, and pcAnywhere, a Symantec spokesman said. The week of January 9, the hackers released the code to a 2006 version of Norton Utilities and said they planned to release code to its antivirus software January 17. It was unclear why the source code was being released 6 years after the theft. The

spokesman said the 2006 attack presented no threat to customers using the most recent versions of Symantec's software. Yet, an analyst with ITIC who helps companies evaluate security software, said Symantec's customers should be concerned about the potential for hackers to use the stolen source code to figure out how to defeat some protections in Symantec's software. Symantec said earlier in January its own network was not breached when the source code was taken. However, the spokesman said January 17 an investigation into the matter revealed the company's networks were compromised. He also said customers of pcAnywhere, a program that facilitates remote access of PCs, may face "a slightly increased security risk" as a result of the exposure.
Source: http://www.reuters.com/article/2012/01/17/us-symantec-hackers-idUSTRE80G1DX20120117

48. *January 11, Cisco* – (International) **Cisco security response: Wi-Fi protected setup PIN brute force vulnerability.** On December 27, the U.S. Computer Emergency Readiness Team released Vulnerability Note #723755, describing a vulnerability that exists in the Wi-Fi Alliance Wi-Fi Protected Setup (WPS) protocol, also known as Wi-Fi Simple Config, when devices are operating in PIN External Registrar (PIN-ER) mode. Devices operating in PIN-ER mode allow a WPS capable client to supply only the correct WPS PIN to configure their client on a properly secured network. A weakness in the protocol affects all devices that operate in the PIN-ER mode, and may allow an unauthenticated, remote attacker to brute force the WPS configuration PIN in a short amount of time. Now, Cisco announced exploit code and functional attack tools that exploit the weakness within the WPS protocol have been released. The vulnerability is due to a flaw that allows an attacker to determine when the first 4-digits of the 8-digit PIN are known. The eighth digit of the PIN is utilized as a checksum of the first 7 digits and does not contribute to the available PIN space. Because the PIN space has been significantly reduced, an attacker could brute force the WPS pin in as little as a few hours. While the affected devices implement the WPS 1.0 standard that requires that a 60-second lockout be implemented after three unsuccessful attempts to authenticate to the device, this does not substantially mitigate this issue as it only increases the time to exploit the protocol weakness from a few hours to at most several days. It is Cisco's recommendation to disable the WPS feature to prevent exploitation of this vulnerability.
Source: https://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps

For more stories, see items **12**, **13**, **15**, and **51**

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. *January 18, Green Bay Press-Gazette* – (Wisconsin) **WYDR The Drive back on the air after power failure.** The frequency for radio station WYDR The Drive in Neenah, Wisconsin, went dead January 18 for several hours after a power failure at its transmitter site resulting from the cold weather. The classic rock station that broadcasts to the Fox Cities was silent at about 6:15 a.m. but was live again at around 11 a.m. Its sister stations in Green Bay, 99.7 and 101.9, and the online stream were unaffected. The power outage resulted from freezing temperatures in the transmitter building, according to the station.
Source:
http://www.greenbaypressgazette.com/article/20120118/GPG0101/120118067/WYDR-Drive-off-air-because-power-outage?odyssey=mod|defcon|text|GPG-News

50. *January 18, Raleigh News & Observer* – (North Carolina) **Time Warner Internet blackout not SOPA related.** A major Internet outage kept Time Warner customers across North Carolina offline the morning of January 18. Internet services were restored, as of 9:09 a.m., a Time Warner spokesman said. "We did some maintenance overnight. An issue affected both Internet and TV services. The outage began around 6 a.m.," the Time Warner spokesman said.
Source: http://www.newsobserver.com/2012/01/18/1787136/time-warner-internet-blackout.html

51. *January 18, Chillicothe Gazette* – (Ohio) **Weather, water disrupt TV, Internet services.** Storms January 17 resulted in Horizon warning Ohio customers about service outages. A power outage in Columbus caused WCMH-TV (Channel 4, NBC) and WBNS-TV (Channel 10, CBS) to lose power at their transmission towers. Horizon customers January 17 lost those two channels until power could be restored at the tower location, which was expected to happen by the morning of January 18. The channel outages also impacted DirectTV subscribers. Internet service also could be affected because of a broken water line in a Columbus building that houses Internet connection equipment for several Internet service providers around Ohio. A Horizon spokesman said January 17 that power to that building had to be shut off until the water line could be fixed. Auxiliary power had to be used, but had the potential to shut off and cause Internet service interruptions.
Source: http://www.chillicothegazette.com/article/20120118/NEWS01/201180325

52. *January 17, Rochester Democrat and Chronicle* – (New York) **WXXI radio tower damaged.** Repairs to the damaged WXXI radio tower in Rochester, New York, took the AM station off the air for several hours January 17. WRUR-FM (88.5) remained on the air while WXXI-AM (1370) was off, a spokeswoman for the public radio station said. She gave no specifics on the damage to the tower. A statement on the station's Web site shortly before 1 p.m. said, "AM 1370 is now back on the air. We will continue broadcasting on FM 88.5 today, through the end of All Things Considered. At 6 p.m., WRUR will resume its regular programming."
Source:

http://www.democratandchronicle.com/article/20120117/NEWS01/120117014/WXXI-radio-tower-damaged?odyssey=nav|head

53. *January 17, WHNS 21 Greenville* – (South Carolina) **Weather radio transmitter broadcasting again.** The weather radio transmitter in South Carolina that was damaged the week of January 9 was back on the air January 17, according to the National Weather Service (NWS). Officials said the transmitter on Paris Mountain in Greenville County, which broadcasts on a frequency of 162.55 megahertz, experienced a major hardware failure. On January 17, the NWS said a temporary antenna was brought in to provide service until the main antenna can be replaced. They said the temporary transmitter was broadcasting, but only at half the power. The NWS said the main antenna will be replaced sometime late this winter.
Source: http://www.foxcarolina.com/story/16539751/weather-radio-transmitter-broadcasting-again

For more stories, see items **13** and **45**

[Return to top]

Commercial Facilities Sector

54. *January 18, WLKY 32 Louisville* – (Kentucky) **East Louisville residents clean up storm damage.** Businesses and residents in east Louisville, Kentucky, were busy January 18 cleaning up damage left behind by severe weather January 17. The tennis club at Springhurst was temporarily closed after taking a direct hit from one of the tornadoes. Winds tore one wall of the building completely off, leaving siding, roofing, and insulation everywhere. At the tennis club, the courts were packed at the time the tornado came through, with roughly 50 people on them. However, owners got everyone off them and into safety before it officially hit. The club was just a portion of the 4-mile path the National Weather Service said the tornado took. In other areas of eastern Jefferson County, trees were uprooted and utility poles were toppled, leaving lines dangling. It was all the result of a tornado packing winds in the 95 mph range.
Source: http://www.wlky.com/news/30238444/detail.html

55. *January 18, Softpedia* – (International) **Government and military members exposed after David Morgan hack.** A hacker managed to bypass the security mechanisms implemented by online clothing and accessories store David Morgan, leaking usernames, represented by e-mails, and password hashes, Softpedia reported January 18. The hacker posted a number of 6,000 credential sets on Pastebin, but he claims he obtained more than 24,000 in total. The hacker warned a lot of the e-mail addresses utilized as usernames end in .mil and .gov domain extensions which is an indication that members of the government and military may be exposed as a result of the hack. The hacker identified 71 .mil and 76 .gov email addresses among the leaked data. Besides the military and government e-mail addresses, the leak also contains many usernames represented by company e-mails, which may be used to launch targeted social engineering attacks.

Source: http://news.softpedia.com/news/Government-and-Military-Members-Exposed-After-David-Morgan-Hack-247111.shtml

56. *January 17, CNN* – (California) **Accused California salon shooter to be arraigned Wednesday.** A man who allegedly shot his ex-wife and seven other people to death in the deadliest shooting in Orange County, California, was indicted and scheduled to be arraigned January 18, prosecutors said. The suspect was indicted January 17 on multiple charges related to the October 12 shooting at the Salon Meritage hair salon in Seal Beach, the Orange County District Attorney's office said. The suspect faces eight felony counts of special circumstances murder for committing multiple murders, and one felony count of attempted murder, officials said. Prosecutors previously said they will seek the death penalty. The suspect and his ex-wife were battling over custody of their son, and the dispute was the motive in the shooting, the Orange County District Attorney said in October.
Source: http://www.cnn.com/2012/01/17/justice/california-shooting-indictment/index.html?hpt=us_c2

57. *January 17, Orlando Sentinel* – (Florida) **Man who left pipe bomb in Ocoee park arrested, cops say.** Police in Ocoee, Florida, arrested a man accused of planting a pipe bomb at the city's Central Park in July 2011, the police department said January 17. A city parks services worker found the pipe bomb, police said, under a pavilion. The worker took the device to the police department. Officers called in an Orange County Sheriff's Office bomb squad, which detonated the bomb. Investigators at the time said the device was either live or had been live "at one time." Investigators later identified the suspect as the man responsible for the bomb. He faces charges of possession of or manufacturing of a destructive device.
Source: http://www.orlandosentinel.com/news/local/orange/os-pipe-bomb-arrest-ocoee-central-park-20120117,0,7127131.story

For another story, see item **29**

[Return to top]

National Monuments and Icons Sector

58. *January 17, Dayton Beach News-Journal* – (Florida) **Forest Service and firefighters battle new fires.** Two new fires sprang up January 17 in Volusia County, Florida, bringing to the total number of fires being monitored to 10. Florida Forest Service (FFS) and Volusia County firefighters were able to quickly get one fire under control, containing it to about 1 acre. Shortly afterwards, an individual with the forest service was driving along U.S. 92 west of Daytona Beach when he saw a column of smoke in the woods and reported it. The fire was burning in a wooded area perilously close to many homes. This time, firefighters with the city of Daytona Beach helped the FFS and Volusia County firefighters control the fire and protect the homes. Working in thick smoke, forest service bulldozer operators quickly laid down a wide lane around the fire and estimated it was contained at between 1 and 2 acres. Meanwhile, firefighters continue to monitor the fires burning elsewhere in Volusia County. At many locations,

firefighters stayed on duty overnight to prevent flareups.
Source: http://www.news-journalonline.com/breakingnews/2012/01/forest-service-and-firefighters-battle-new-fires.html

59. *January 16, WKMG 6 Orlando* – (Florida) **Arson ruled out in fire that toppled 'The Senator' at Big Tree Park.** Fire officials said arson is not to blame in a fire that toppled "The Senator," one of the oldest cypress trees in the world, which was reduced to a stump January 16 at Big Tree Park in Seminole County, Florida. Investigators initially said arson was a possibility because a pile of twigs was found at the base of the tree, there had not been recent lightning strike, and no power lines are located nearby. The official cause is not yet known, and an investigation is ongoing. An arson investigator said the possible cause was a lightning strike from a few weeks ago. The tree, named after a Florida senator who in 1927 donated the property on which the landmark sits, was about 120 feet tall and its trunk had a diameter of nearly 18 feet. It was the main attraction in the park dedicated in 1929. The tree had reached a height of 165 feet before a 1925 hurricane lopped off its top. Afterward, lightning rods were installed to protect the tree. More than a dozen firefighters were at the park when the fire occurred but hoses and water from a helicopter could not save the tree.
Source: http://www.clickorlando.com/news/Arson-ruled-out-in-fire-that-toppled-The-Senator-at-Big-Tree-Park/-/1637132/8136768/-/tp6dmc/-/

[Return to top]

Dams Sector

60. *January 16, 90.5 FM Pittsburgh* – (Pennsylvania) **Three Rivers locks and dams in need of repair.** The head of the Port of Pittsburgh Commission said massive infrastructure upgrades are needed for the Three Rivers' locks and dams. In an appeal for funding to the Pennsylvania House Democratic Policy Committee the week of January 9, the port commission executive director said each river has problems. "The Lower Mon will need about $100 million a year for the next 10 years. That project is already eight years behind," said the director. "The Ohio River needs an authorization through Congress. The Allegheny River, they have begun effectively to close Locks 8 and 9," and Locks 5, 6, and 7 will not be repaired, if damaged. He said the American Society of Civil Engineers gave the 17 locks and dams in the port system a report card with three F's, seven D's, five C's, and two B's — a combined "grade point average" of just 1.35. He called on the legislature and the governor to restore state funding to the port system. The budget line item for the Port of Pittsburgh completely vanished from 2010 to 2011, leaving the port bereft of $738,000. The port now gets about half its funding from the federal government, and half from levies on businesses. In addition to asking for direct state aid, he asked legislators to support a proposal that would set up a $12-24 million yearly fund for "intermodal" transportation projects. According to the director, the port directly sustains 45,000 jobs and indirectly supports 155,000 jobs, generating about $1 billion in state and local tax revenue each year. He said the region's steel, coal, and chemical industries rely heavily on the rivers to do business.
Source: http://www.essentialpublicradio.org/story/2012-01-16/three-rivers-locks-dams-need-repair-9900

For another story, see item **33**

[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