Homeland Security

Daily Open Source Infrastructure Report for 19 January 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- The New York Times reports that on January 14 the Department of Homeland Security moved to increase random checks for explosives at American airports after officials cited a heightened concern over possible terror plots against the aviation system by al Qaeda operatives. Counterterrorism officials said the threat information was vague and did not specify a particular target or date. (See item **21**)
- According to the Associated Press, a chemical spill at the Clackamas County Dental Clinic in Oregon City, Oregon sent at least 10 people to three area hospitals on January 14. The spilled chemical was formocresol, a solution used in dental work. (See item **41**)

Fast Jump Menu

Energy Sector

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

1. *January 15, Reuters* – (International) **Security at oil facilities in east India tightened.** India has deployed additional forces to guard energy facilities including an oil refinery in the eastern state of Bihar after police found maps of such units with a suspected militant from Bangladesh. “We are investigating how he managed to get

maps of key oil installations," a senior police officer said on January 15. The suspected militant was arrested on on January 13, police said. State-run Indian Oil Corp (IOC.BO) has 14 key oil facilities in the state, including a 120,000 barrels per day refinery at Barauni, depots and plants to fill cooking gas in cylinders. The move comes weeks after intelligence agencies said militants may target oil refineries and nuclear facilities. "We have been informed that oil refineries and other key government installations could be targets," a senior police officer in the district where the Barauni refinery is located told Reuters.
Source:
http://www.reuters.com/article/idUSSGE60E08B20100115?type=marketsNews

2. *January 14, Honolulu Adverstiser* – (Hawaii) **Workers injured in underground blast on Fort Street Mall; power restored.** Two Hawaiian Electric Company (HECO) workers were injured Thursday morning, one seriously, in an underground explosion that left parts of Downtown Honolulu without power for about five hours. Power was restored at 3:15 p.m. The explosion took place in an electrical vault on Fort Street Mall. An employee of the city's Emergency Services Department said paramedics were dispatched at 10:19 a.m. Shortly after the explosion, traffic lights were reported going out in several sections of Downtown. A HECO spokesman said about 1,100 customers were without power in the Downtown area bounded by Bethel to Richards streets and Beretania to Merchant streets.
Source:
http://www.honoluluadvertiser.com/article/20100114/BREAKING01/100114038/Workers+injured+in+underground+blast+on+Fort+Street+Mall++power+restored

3. *January 14, Ledger Independent* – (Kentucky) **Over three miles of copper wire stolen from Duke Energy.** At least 10 reports of theft of copper wire from Duke Energy have come in since November 27, with the most recent report on January 14, said a detective with the Brown County Sheriff's Office. He said each time a theft is reported, another 2,000 to 3,000 feet of wire is missing. In total, more than three and a half miles of copper wire has been stolen. He said the perpetrator appears to be climbing telephone poles then using bolt cutters to cut down numbers two and four neutral copper wire. To climb the poles, typically a person must have specific footwear pole climbers use. Though Duke Energy is not the only electric provider for Brown County, so far it is the only one to be affected by the thefts. A spokesperson for Duke Energy said the copper wire is replaced with aluminum wire. So far, no one has reported outages from the cutting of the wire, but she said removing the wire from the poles poses a hazard to all. The detective said some people have reported suspicious activity, but the lapse between the time of the theft and the reports make it difficult for police to obtain the information they need for the investigation. They both encouraged anyone who sees a person on a pole who does not have a marked Duke Energy truck nearby or the Duke Energy hard hat to call police.
Source: http://www.maysville-online.com/news/local/article_5f58f4c8-0199-11df-8826-001cc4c002e0.html

4. *January 14, KVUE 33 Austin* – (Texas) **Vandalism suspected in gas service outage.** Austin Police say someone intentionally shut off the gas service to West Lake Hills on January 12. It may not be the first time this has happened. Thousands went without warm water or heat. Texas Gas Service employees believe it was intentional because of what they found at the regulator station at Loop 360 and Westlake Drive. "They determined that somebody purposefully closed the valve," an APD corporal said. Two weeks ago, the same thing happened at another regulator station three miles down Loop 360 at the Gables apartment complex. Someone turned off the gas in the early morning hours of January 2nd. However, at the time the gas service employees did not think it was criminal. The more than 400 customers remember that day very well. Investigators are now trying to determine if the two cases are related. A Texas Gas Service spokesperson says they are changing the locks and reviewing other security features. On the afternoon of January 14, KVUE witnessed crews putting "no trespassing" signs on the regulator stations.
   Source: http://www.kvue.com/news/Vandals-suspected-in-gas-service-cut-off-81580307.html

5. *January 13, WCVB 5 Boston* – (Massachusetts) **Coast Guard ramps up security for Yemen LNG.** Coast Guard officials reassured Massachusetts lawmakers that they are ramping up security ahead of a scheduled delivery of liquefied natural gas from Yemen next month. Lawmakers said a Coast Guard captain told them in a closed-door meeting Wednesday that he will not let the tanker make its delivery in Everett unless he is convinced all security measures have been taken. U.S. officials are considering whether to call for additional security measures for shipments of liquefied natural gas originating in Yemen. The Massachusetts house speaker said his top worry is that a bomb could be smuggled on and detonated as the tanker passed by populated areas or under the Tobin Bridge. A U.S. Senator from Massachusetts also attended the meeting and said state and federal officials should be thinking long term about safer methods to deliver natural gas, other than bringing the giant tankers so close to populated areas like Everett, Chelsea, and nearby Boston neighborhoods. A Coast Guard spokesman said the next delivery from Yemen is not scheduled until late February, and the captain will not give the tanker permission to enter the port until he is convinced all security measures have been taken.
   Source: http://www.thebostonchannel.com/news/22231859/detail.html

[Return to top]

Chemical Industry Sector

6. *January 14, KHTS 1220 Santa Clara* – (California) **Chemical spill temporarily closes northbound 5.** A chemical spill temporarily closed the northbound I-5 near highway 138 the afternoon of January 13. The California Highway Patrol reported that bags of high calcium hydrated lime spilled over a 200-foot section of the highway. One officer was exposed to the chemicals but was treated at the scene. L.A County Hazmat responded to the spill but Caltrans finished the cleanup which took about three hours to complete. According to Graymont.com, a company that manufactures lime, hydrated

lime is used in a variety of industrial applications including water treatment, as an anti-stripping agent in asphalt, and in soil stabilization.
Source:
http://hometownstation.com/index.php?option=com_content&view=article&id=19006:sigalert-northbound-i-5-closed-past-highway-138&catid=26:local-news&Itemid=97

7. *January 12, WCBD 2 Charleston* – (South Carolina) **Ammonia leak contained in Walterboro.** A small ammonia leak was reported around 12:20 the afternoon of January 12 at the Cummings Oil Company in Walterboro. The operations chief with the Colleton County Fire-rescue says hazmat crews have been able to contain the leak to a small area within the parking lot of the business. A clean up contractor is expected to complete the work the evening of January 12. Some of the material went into a nearby storm drain so the hazmat team set up equipment to monitor the situation. Officials say the leak began when employees were doing maintenance on a tank which contained anhydrous ammonia. No one was injured and there was no evacuation or road closing to nearby residents or motorists.
Source:
http://www2.counton2.com/cbd/news/local/article/developing_ammonia_leak_in_walterboro/102531/

For another story, see item **31**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *January 15, Associated Press* – (National) **Purdue researchers test new nuclear power plant design to ensure it stands up to strong quakes.** Purdue University researchers are testing a new design for nuclear power plants to make sure it can survive strong earthquakes. The Purdue team will test components of an "enhanced shield building" designed by Westinghouse Electric Co. to contain the main system components of nuclear power plants. That building consists of an inner steel-wall containment vessel and an outer radiation shield made using a technology called steel-concrete-composite construction. Conventional design for those buildings use reinforced concrete strengthened with steel bars. But the new design uses a sandwich of steel plates filled with concrete. The Purdue researchers are concentrating on how seismic forces affect the concrete-filled walls, the connection between the walls, and the structure's reinforced-concrete foundation.
Source: http://www.baltimoresun.com/business/sns-ap-us-purdue-nuclear-design-indiana,0,3112882.story

9. *January 14, New Jersey Star Ledger* – (New Jersey) **Nuclear agency sweeps up radioactive equipment from Rahway company.** The National Nuclear Security Administration swept into a Rahway, New Jersey, warehouse the week of January 4 to secure Cesium-137, a radioactive substance, from unused medical equipment. The agency did not release any information about the operation until a week later, once the

equipment, medical irradiator machines, was treated and safely housed thousands of miles away, west of the Mississippi River. It also did not give the name or address of the Rahway company in order to protect it from those trying to illegally acquire radioactive substances. The Cesium was only about the size of two rolls of quarters, but in the wrong hands, it could be used in an explosive that could cause billions of dollars in economic damage and possible injuries and deaths for civilians, according to a deputy director for the government agency. "Properly disposing of more than 3,000 curies of Cesium eliminates the threat this material poses if lost or stolen and used in a dirty bomb," said the administrator of the federal agency in a statement January 14.
Source: http://www.nj.com/news/local/index.ssf/2010/01/nuclear_agency_sweeps_up_radio.html

[Return to top]

Critical Manufacturing Sector

10. *January 15, WHIO 7 Dayton* – (Ohio) **Second machine fire in six months flares at Kettering plant.** A fire started at the Tenneco plant on January 14. The blaze reportedly started in a machine at the plant. Another machine fire brought four departments to the scene back in August. Tenneco, Inc. manufactures automotive parts.
Source: http://newstalkradiowhio.com/localnews/2010/01/second-machine-fire-in-six-mon.html

[Return to top]

Defense Industrial Base Sector

11. *January 15, Naval Open Source Intelligence* – (National) **Raytheon's Standard Missile-6 completes guided test vehicle launch.** Raytheon Company's Standard Missile-6 successfully completed its fourth guided test vehicle launch, clearing the way for the missile's at-sea testing this year. "All GTV engineering test objectives were met, demonstrating the SM-6's capabilities in this critical engagement," said Raytheon's vice president of Naval Weapon Systems. "With its over-the-horizon protection, SM-6 will provide the surface Navy with an increased battlespace against anti-air warfare threats. We now move forward with initial operational capability flights of this extended-range AAW system."
Source: http://nosint.blogspot.com/2010/01/raytheons-standard-missile-6-completes.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence)

12. *January 13, Reuters* – (Texas) **U.S. uses CT scans to check out nuclear stockpile.** The same type of scanner used to peer into the body to detect cancers will be put to an even more delicate use — checking on the viability of the nation's aging nuclear stockpile, the National Nuclear Security Administration said on Wednesday. The agency, part of the U.S. Department of Energy, said it has begun using computed

tomography or CT scans — an advanced type of X-ray — to detect aging defects on critical components in the nation's nuclear weapons arsenal. The high-resolution scanner, called the CoLOSSIS (Confined Large Optical Scintillator Screen and Imaging System), was built by scientists at Lawrence Livermore National Laboratory. It is used to scan weapons components to look for signs that nuclear weapons have degraded in the past 30 to 40 years since they were first built. "There are up to 6,000 components in a nuclear warhead. Those can be anywhere from very small to relatively large. I don't think we are talking about passing the whole thing to the scanner," said the director of public affairs at the National Nuclear Security Administration. The work is typically done at the Pantex Plant, where the NNSA assembles and disassembles nuclear weapons as part of its stockpile stewardship mission. Before the scanner, the team at Pantex would take a weapon out of service and inspect it. "We would have to cut it, take it apart completely and make everything completely useless. You couldn't re-weld them back together," an expert said. "What this allows us to do is take a component and without damaging it — find out what's inside and outside." The first user of the CoLOSIS will be Los Alamos National Laboratory, which will test the Air Force's B61 gravity bomb, checking components for signs of aging or manufacturing defects. Source: http://www.reuters.com/article/idUSTRE60C6N220100113

For another story, see item **57**

[Return to top]

Banking and Finance Sector

13. *January 15, IDG News Service* – (International) **UK defendants await sentencing in carding scheme.** Two U.K. men have pleaded guilty to charges related to the infamous DarkMarket payment-card fraud ring busted by authorities in October 2008, according to British police. The two men both pleaded guilty to conspiracy to defraud in Blackfriars Crown Court in London on January 14. DarkMarket was a highly organized, password-protected online forum where criminals worldwide could buy and sell credit card numbers, a practice known as "carding." Since its shutdown, more than 60 people have been arrested by law enforcement agencies in the U.K., U.S., Germany, Turkey and other countries. The 33 year old suspect was an "itinerant loner" who was allegedly observed selling lists of credit cards near the Java Bean Internet Cafe in Wembley where he frequently accessed the DarkMarket site, according to the Serious Organised Crime Agency (SOCA). He used a memory stick to carry data around and seemed to think using Internet cafes would help shield his activities, SOCA said. The 66 year old suspect was arrested in December 2008 after investigators found he was allegedly running a counterfeit credit card factory, SOCA said. This suspect, a retiree who lived in Doncaster, England, allegedly had details for more than 2,000 credit cards in his home along with a "suite of images and logos" needed to produce fake cards. Source: http://www.networkworld.com/news/2010/011510-uk-defendants-await-sentencing-in.html?hpg1=bn

14. *January 15, United Press International* – (National) **FDIC head: 'Shadow banks' need regulation.** Regulators and the market failed to control the "shadow banking system," the head of the Federal Deposit Insurance Corp. said in Washington. In testimony before the Financial Crisis Inquiry Commission, the chairman said the last wave of federal regulation after the savings and loan crisis 20 years ago encouraged the growth of financial institutions outside the regulators' reach. These institutions became so complex and large they could not simply declare bankruptcy when they got into trouble, she said. They are also outside FDIC receivership. The chairman said what is needed now is a "holistic" regulatory system. "To be sure, we can improve oversight of insured institutions, but if reforms only layer more regulation upon traditional banks, it will just create more incentives for financial activity to move to less regulated venues," she said. "Such an outcome would only exacerbate the regulatory arbitrage that fed this crisis. If that occurs, reform efforts will once again be circumvented, as they were over the past two decades."
Source: http://www.upi.com/Top_News/US/2010/01/15/FDIC-head-Shadow-banks-need-regulation/UPI-63841263538627/

15. *January 15, IDG News Service* – (International) **Romanian faces five years in prison for phishing scheme.** A Romanian national pleaded guilty on January 14 to a charge related to a phishing operation that sought to defraud customers of banks such as Citibank and Wells Fargo, and of Web sites such as eBay. The 28 year old, of Galati, Romania, could face up to five years in prison when he is sentenced on April 5 in U.S. District Court for the District of Connecticut, according to the U.S. Department of Justice. He pleaded guilty to a single charge of conspiracy to commit fraud related to spam. The suspect and another Romanian were accused of setting up fake Web sites in order to steal passwords and sensitive financial information. They also were allegedly passing payment card details to others who would then make fraudulent cards. A third Romanian co-conspirator was the first foreign national convicted in the U.S. of phishing and was sentenced in March 2009 to more than four years in prison. The main the 28 year old admitted using software to collect e-mail addresses in order to send spam that would then try to entice people into browsing one of the fake Web sites.
Source:
http://www.pcworld.com/businesscenter/article/186981/romanian_faces_five_years_in_prison_for_phishing_scheme.html

16. *January 15, Gaithersburg Gazette* – (Maryland) **Few state banks have repaid TARP money to Treasury.** Only three of the 20 Maryland banks that sold stock to the federal government through the Treasury Department's Troubled Asset Relief Program have repaid at least part of the money, according to federal figures. The CEO of Shore Bancshares said the organization was "moving on," and he did not want to comment beyond what the company said in a statement in March. Then, the CEO cited rule and image changes for the quick repurchase. "The representation made by the Treasury concerning TARP was that the program was designed to attract broad participation by healthy institutions, and that our participation in the program was important to restore confidence in our financial system and ensure that credit continue to be available to consumers and businesses," the CEO said in the statement. "Over the past few months,

however, it has become clear to us that the public, including many members of Congress, view institutions that participated in TARP as having done so because they are weak. ... We now believe that our participation in TARP puts us at a competitive disadvantage." The only other Maryland bank that has repaid its TARP funds is Old Line Bancshares, according to Treasury figures as of January 12. Allowing banks to repay TARP funds so soon may backfire, said a bank analyst at Institutional Risk Analytics of Torrance, California, in a recent report. Despite signs of economic recovery, many banks may continue to experience higher losses this year from bad loans, he said.
Source: http://www.gazette.net/stories/01152010/businew175256_32565.php

17. *January 15, Associated Press* – (National) **Holder to look into FBI report of mortgage fraud.** The Attorney General on January 14 told a commission investigating the financial crisis that he would find out whether anything was done in response to an FBI warning in 2004 of an "epidemic of mortgage fraud" that could plunge the country into financial collapse. He also said the diversion of hundreds of Justice Department and FBI officers to terrorism-related duties after the September 11, 2001, terror attacks may have made it harder for his agency to investigate the kind of risky banking practices that led to the nation's financial meltdown in 2008. But he said that fighting white-collar crime had become a top priority for him and that more resources were being devoted to such cases. He testified at the second day of hearings by the Financial Crisis Inquiry Commission, a 10-member panel created by Congress to explore the causes of the economic collapse. The Commission Chairman grilled him over a September 4, 2004, warning from a top FBI official about "an epidemic of mortgage fraud coursing across this country" and the dire crisis that could occur if it were left unchecked. That was four years before the financial meltdown on Wall Street that led to unprecedented government bailouts of some of the nation's largest banks and financial institutions.
Source: http://www.philly.com/philly/business/81649327.html

18. *January 14, DarkReading* – (New Hampshire) **Lincoln National discloses breach of 1.2 million customers.** Lincoln National Corp. (LNC) recently disclosed a security vulnerability in its portfolio information system that could have compromised the account data of approximately 1.2 million customers. In a disclosure letter sent to the attorney general of New Hampshire January 4, attorneys for the financial services firm revealed that a breach of the Lincoln portfolio information system had been reported to the Financial Industry Regulatory Authority (FINRA) by an unidentified source last August. The company was planning to issue notification to the affected customers on January 6, the letter says. The letter does not give technical details about the breach, but it indicates the unidentified source sent FINRA a username and password to the portfolio management system. "This username and password had been shared among certain employees of [Lincoln Financial Services] and employees of affiliated companies," the letter says. "The sharing of usernames and passwords is not permitted under the LNC security policy." Upon further investigation, Lincoln found another of its subsidiaries, Lincoln Financial Advisers, was using shared usernames and passwords to access the portfolio information management system, the letter states. In

the end the company found a total of six shared usernames and passwords, which were created as early as 2002. The forensic team that investigated the breach found no evidence that the data had been used outside of the company, either by hackers or former employers, according to the letter.
Source:
http://www.darkreading.com/vulnerability_management/security/privacy/showArticle.jhtml?articleID=222301034

For another story, see item **57**

[Return to top]

Transportation Sector

19. *January 15, Olympian* – (Washington) **Sea-Tac first to use new bird-tracking radar.** Sea-Tac Airport the week of January 11 became the nation's first airport to put an advanced bird-tracking radar into service in the airport vicinity. The new radar, developed in partnership with the University of Illinois and the Federal Aviation Administration, allows airport wildlife experts to view in real time bird activity as they drive around the airport. The airport has been demonstrating early versions of the avian radar since 2007. Tracking birds is important on and near the airport because birds can damage planes taking off and landing. "This technology will give us situational awareness of the entire airfield day or night. It will be like wearing a huge pair of binoculars," said the airport's wildlife biologist. Knowing where birds are flying helps air traffic controllers delay takeoffs and landings until the birds have flown past and gives wildlife patrol officers the location of flocks that they can scare away.
Source: http://www.theolympian.com/business/story/1102220.html

20. *January 15, Philadelphia Daily News* – (Pennsylvania) **Thousands of birds to be killed at Pa. airport.** Officials plan to poison as many as 15,000 European starlings at University Park Airport more than three years after a commercial airline struck a flock there. The U.S. Department of Agriculture (USDA) plans to use a pesticide on the starlings to help reduce the bird-strike risk, the airport director said. On August 19, 2006, a commercial airliner ran into a flock after takeoff, suffered engine damage, and had to return to the airport. The Federal Aviation Administration's wildlife strike database reports that the Air Wisconsin-owned Canadair jetliner, flying for US Airways, sustained "substantial" damage, the Centre Daily Times reported. A USDA spokeswoman said that the starling flock found in the area had about 15,000 to 20,000 birds, and that the department planned to kill about 90 percent of them.
Source: http://www.philly.com/philly/news/new_jersey/81649687.html

21. *January 15, New York Times* – (National) **Possibility of plots prompts more checks for explosives at airports.** The Department of Homeland Security moved January 14 to increase random checks for explosives at American airports after officials cited a heightened concern over possible terror plots against the aviation system. Counterterrorism officials said that recent intelligence tips had hinted at a planned

attack by Qaeda operatives, but that the threat information was vague and did not specify a particular target or date. Still, after failing to anticipate the attempted Christmas Day bombing of a Northwest Airlines flight, government officials said they wanted to take every precaution. "We must remain vigilant about the continued threat we face" from Al Qaeda," the Homeland Security Secretary said in a statement. "We are facing a determined enemy and we appreciate the patience of all Americans and visitors to our country, and the cooperation of our international partners as well as a committed airline industry." The measures will include random checks with explosive-detection devices of passengers or baggage at locations around some American airports, not just at security checkpoints, one Homeland Security Department official said. The devices search for trace amounts of explosives as a sign that someone might be carrying a bomb. Air marshals will also more frequently board flights on certain unidentified routes, officials said. Canine teams and so-called behavior detection officers — which have been deployed in larger numbers since the December 25 episode — will continue to patrol airports, looking for suspicious activity or explosives. Three American counterterrorism officials declined the evening of January 14 to say what prompted the new travel advisory. But they suggested that they had seen an increase in tips about a possible attack from Al Qaeda in the Arabian Peninsula, the Yemen-based group that claimed credit for the failed December 25 plot.
Source: http://www.nytimes.com/2010/01/15/us/15secure.html

22. *January 14, KOAT 7 Albuquerque* – (New Mexico) **Sheriffs investigate train robberies.** Investigators with the Valencia County Sheriff's Department are looking for those responsible for breaking into several railcars. Detectives do not have any leads, and have no idea who could be doing this. All they know is that these break-ins occur when a train stops to let another train pass. It's a busy a shift for BNSF crews in the rail yard, and investigators say it is even busier for the thieves waiting near the tracks. "It's unknown when the train is going to stop, but apparently these individuals have an idea," said a Valencia County Sheriff. "That's where they're taking the merchandise off the train." Investigators believe the thieves are breaking the locks on the cars to get their hands on merchandise that can be stolen and easily re-sold. An official with BNSF operations said the most recent theft was copper on the cars. Officials are hoping the theft was an isolated incident, but this is not the first time BNSF has had thieves break into the railcars.
Source: http://www.koat.com/news/22242066/detail.html

23. *January 13, Associated Press* – (Florida) **Cleaning crews find threatening letter on parked US Airways jet.** Authorities say a cleaning crew found a threatening letter on a parked US Airways aircraft, but no explosives or other dangers were discovered. A spokesman for Fort Lauderdale-Hollywood International Airport says a member of the crew came across the note early the morning of January 11. The plane had arrived hours earlier from Charlotte, and no passengers were aboard. The spokesman said the note said something about damaging the plane, but he did not specify the exact message. Security officials used dogs to check the plane. The Transportation Security Administration says the plane was cleared and later returned to Charlotte as scheduled.

Source: http://www.usatoday.com/travel/flights/2010-01-13-us-airways-threat-note_N.htm

24. *January 12, Los Angeles Times* – (California) **Safety, traffic concerns raised when 3.5-mile-long freight train rolls through L.A. basin.** An apparently unprecedented super freight train extending some 3.5 miles rolled through Southern California over the January 9 weekend, catching state regulators off guard and prompting concerns about potential safety risks and traffic delays. Union Pacific said the train was a test of equipment and ways to improve operating efficiency, but that the company does not have plans to run such trains regularly. Some officials are worried it may be a harbinger. "I will be asking a lot more questions," said a Democratic representative whose San Gabriel Valley district includes part of the train route. "If they're testing to increase the size of trains in L.A., I have a problem with that." The state Public Utilities Commission raced a team of personnel to Imperial County on January 9 to monitor the train as it wound its way toward the Inland Empire. The train originally left Texas on January 8 and reached its ultimate destination, a large intermodal facility near the Port of Long Beach, on January 10. "We were quite concerned about it, which was why we scrambled our people to be out there Saturday to essentially find out what was going on," said the supervisor of rail safety at the state agency. There are no state or federal limits on the length of trains or requirements to notify agencies about unusually long train configurations, officials said. Union Pacific said it did alert local federal regulators, who observed the train's movement. In addition to concerns about lack of notice to state authorities, who regulate grade crossings, the supervisor said his agency wanted to ensure the massive train had adequate braking capacity and officials were on hand in case of extended delays for motorists and emergency vehicles, especially if the train was forced to stop for some reason.
Source: http://latimesblogs.latimes.com/lanow/2010/01/safety-traffic-concerns-raised-when-35mile-freight-train-rolls-through-la-basin.html

25. *January 11, Progressive Railroading* – (Georgia) **CSXT, Georgia team up to bolster rail security.** On January 8, the governor of Georgia announced the state entered into a rail security partnership with CSX Transportation that "represents a model for use by other states." Entitled "SecureNOW," the pact calls for the state and Class I to share information, resources, and security strategies. For example, the Georgia Emergency Management Agency-Office of Homeland Security will access CSXT's network operations workstations, or NOW system, which enables state and local public safety and law enforcement officials to track the location of CSXT trains and rail-car contents in real time. In addition, the Class I will work with state and local law enforcement officials on joint rail security training and preparedness exercises, and provide round-the-clock access to its rail security professionals.
Source: http://www.progressiverailroading.com/news/article.asp?id=22323

For more stories, see items **5**, **6**, and **69**

[Return to top]

Postal and Shipping Sector

See items **44** and **46**

[Return to top]

Agriculture and Food Sector

26. *January 15, KETV 7 Omaha* – (National) **Baby food may be contaminated.** A popular brand of organic baby food may come with bacteria. Consumers have been advised to watch out for all varieties of "Happy Tot Stage 4" and some pouch meals of "Happy Baby Stage 2" with expiration dates between November 2010 and January 2011. The packages can swell and leak, causing food contamination.
Source: http://www.ketv.com/news/22239330/detail.html

27. *January 14, Baltimore Business Journal* – (Maryland) **Congressional Seafood resumes operations.** Congressional Seafood Co., which was cited by the FDA for failing to follow food safety regulations and ordered to stop distributing fish, has regained compliance after a meeting with FDA officials Wednesday. The Jessup, Maryland-based company says it has resumed normal business operations as of Thursday. Congressional Seafood, which distributes fish and shellfish to restaurants and hotels throughout the Baltimore and Washington, D.C. region, had been warned "on numerous occasions," according to the FDA, about failing to comply with safety laws. The FDA cited violations that included failure to document that fish were refrigerated at appropriate temperatures and failure to meet sanitation standards or to keep records of compliance.
Source: http://www.bizjournals.com/baltimore/stories/2010/01/11/daily34.html

28. *January 14, The Packer* – (Florida) **One-third of Florida vegetables lost to freeze.** Preliminary estimates from Florida show 10 consecutive nights of freezes destroyed nearly a third of the state's winter fruit and vegetable production and caused hundreds of millions of dollars in losses. Harvesting remained stopped in many areas as growers wait for warmer weather to see what they can salvage. The severe cold struck all central and south Florida's growing regions, from Plant City's strawberries to vegetables in Immokalee and Naples in southwest Florida to Belle Glade in West Palm Beach County, to Homestead and areas along the East Coast. On January 14, Florida's Agriculture Commissioner toured the Plant City area and planned to visit other areas hit hard by the severe cold. He is expected to seek federal disaster assistance. A spokesman for the Florida Department of Agriculture and Consumer Services, Tallahassee said state officials would receive preliminary damage estimates the week of January 18. The cycle of sub-zero overnight temperatures ended January 13. He said the state expects a minimum of a 30 percent loss in production and millions of dollars in losses.
Source: http://thepacker.com/One-third-of-Florida-vegetables-lost-to-freeze/Article.aspx?articleid=975511&authorid=683&categoryid=122&feedid=215&src=recent

29. *January 14, Sussex Countian* – (Delaware) **Copper thieves have been active on farms throughout the state.** State authorities are asking the public to help them identify thieves who have targeted copper wiring on single pivot irrigation systems on farms throughout Deleware. "A rash of on-farm copper wire thefts has been reported since November 2009," the Secretary of Agriculture said. "This is a serious problem for farmers because the systems are severely damaged when the theft occurs and repairs often cost several thousand dollars." As recently as January 13, state police investigated a theft and criminal mischief to irrigation farm that may have occurred between early December 2009 and January 14. State Police are now experiencing these thefts along Dona's Landing Road, Savannah Road, SR 9 Bayside Drive near White Oak Road and Long Point road east of Dover. The estimated damage and theft of copper is nearly $38,000. Police have seen an increased number of thefts in the East Dover, Magnolia, Felton and Harrington areas of Kent County.
Source: http://www.sussexcountian.com/newsnow/x1560341391/Copper-thieves-have-been-active-on-farms-throughout-the-state

30. *January 14, Minnesota Public Radio* – (Minnesota) **Minn. food company expands voluntary recall.** A Minnesota food company has expanded its voluntary recall after a state inspection found that all products at the company's Coon Rapids facility may have contaminated by bacteria. The Minnesota Department of Agriculture has advised consumers to discard any food made at the Parkers Farm facility. The agency had issued a more limited advisory on January 8. The facility produces peanut butter, cheese, salsa, cream cheese bagel spreads, and other products under several labels, including Parkers Farm, Happy Farms, Central Markets, and others. The state's Department of Agriculture said sampling found that some of the products were contaminated with the bacteria that can cause listeriosis. No illnesses have been reported. A list of recalled products can be found at http://www.mda.state.mn.us.
Source: http://minnesota.publicradio.org/display/web/2010/01/14/food-recall/

31. *January 14, Oregonian* – (Oregon) **Milwaukie company fined $740,400 for safety violations.** Oregon worker-safety officials handed out the state's stiffest fines in more than a decade Thursday, citing a Milwaukie cold-storage company for repeated and willful violations of state safety standards. Americold Logistics, one of five Oregon locations for the Atlanta-based corporation, has 30 days to appeal fines totaling $740,400. The fines — the fourth-highest ever meted out by the agency — encompassed 10 willful violations, four serious repeat violations and 22 other serious violations of the Oregon Safe Employment Act. Most of the penalties stem from the company's system for handling the hazardous chemical anhydrous ammonia, which is considered common in warehouse operations and can be explosive. Americold Logistics' executives said they were notified of the penalties Wednesday. They plan to spend the new few weeks reviewing the list to decide what specific actions they need to take next. The company's website refers to Americold Logistics as the nation's largest provider of temperature-controlled food distribution services.
Source:
http://www.oregonlive.com/clackamascounty/index.ssf/2010/01/milwaukie_company_hit_with_ste.html

[Return to top]

Water Sector

32. *January 14, Water Technology Online* – (International) **Water supplies dangerously low in Haiti after earthquake.** According to United Nations (UN) officials, water supplies in Haitian capital Port-Au-Prince have been cut after a 7.0 magnitude earthquake struck on January 12, Deutsche Presse-Agentur reported. Over 20 international search and rescue teams have been given permission to enter the island nation, the article stated. "All municipal water supplies are reportedly shut off," said a spokeswoman with the UN Office for the Coordination of Human Affairs. Nearly 3.5 million people are estimated to be affected by the earthquake, according to the article. "(What) people need urgently, more than food, is water," said a UNICEF spokesperson. Source: http://watertechonline.com/news.asp?N_ID=73254

33. *January 14, Honolulu Adverstiser* – (Hawaii) **Water-quality violations will cost city $300,000.** The Hawaii State Department of Health on January 13 announced it has reached a settlement with the city regarding the alleged discharge of wastewater from comfort stations at Kualoa Beach Park in late 2005 to early 2007. The Health Department is alleging that the discharges caused high bacteria counts in the nearshore ocean waters, which required warning signs on the beach for several months. The city admitted no liability in settling the case. The settlement requires that the city seek the approvals needed to replace the park's wastewater systems, remove its wastewater by pump truck until the replacement is completed and pay $300,000 to settle permit and water quality violations alleged by the Health Department.
Source:
http://www.honoluluadvertiser.com/article/20100114/NEWS25/1140339/Water-quality+violations+will+cost+city++300+000

34. *January 14, Charleston Gazette* – (West Virginia) **Officials on trail of missing generator switches.** Pratt, West Virginia, town officials are on the trail of two missing transfer switches after the Kanawha County commission president threatened to call in sheriff's deputies. The switches are needed to hook up two emergency generators county officials bought to provide emergency power for Pratt's sewer system in 2008. The generators have never been installed. Town officials discovered there were no transfer switches last month, after a power outage allowed Pratt's sewer pumps to back up, releasing about 30,000 gallons of raw sewage into the environment. County officials confirmed Wednesday that the county had paid for the switches as part of the $57,000 cost of the generators. Pratt turned over operation of the town sewer plant to the Chelyan Public Service District (PSD) the week of January 4. But when officials for Chelyan went to look for the switches so they could install the emergency generators, the switches were nowhere to be found. The president asked the sheriff to investigate. But the chairman of the Chelyan PSD's governing board may have discovered what happened to the switches. He and and Chelyan PSD a board member told county officials on January 12 they were able to track down the former plant manager, who said he gave the switches to an employee at DuPont to figure out how to wire them.

They are trying to track the employee down. Officials for the Chelyan PSD hope to have the switches back by January 16.
Source: http://www.istockanalyst.com/article/viewiStockNews/articleid/3781934#

35. *January 14, Associated Press* – (North Carolina) **Cold weather hits NC city with broken water lines.** The cold weather has broken so many water lines in High Point, North Carolina, that officials are asking residents to conserve water. Multiple media outlets reported Thursday that High Point water customers have used between one million and two million gallons a day more this year than last year. The city public services director says the city has worked on about 30 water main breaks in the past month. The broken lines force the city to push more water through its treatment plant to keep up with the need. That's why High Point is asking residents to conserve water for the next month. The city predicts more problems as the cold temperatures rise. The thawing ground will move, causing new breaks in water lines.
Source: http://www.wlos.com/template/inews_wire/wires.regional.nc/29d7c929-www.wlos.com.shtml

36. *January 13, Empire State News* – (New York) **Greenpoint property owner faces 81-count pollution indictment.** The Kings County district attorney, the New York State Department of Environmental Conservation (DEC) commissioner, and New York City Department of Environmental Protection (DEP) commissioner announced the indictment of a Greenpoint commercial property owner charged with dumping into Newtown Creek. Norman Holding, LLC, and its principle are charged in an 81-count indictment with dumping raw sewage directly into the creek, from three commercial buildings on North Henry St., which the principle rented out to eight businesses. According to the indictment, all three buildings had toilets and sinks connected directly to the underground storm-water drainage system, instead of the municipal sewer system. The defendants are charged with 27 counts of discharging sewage without a state pollution discharge elimination system (spdes) permit, a felony; 27 counts of prohibited discharges, also a felony; and general prohibition against pollution, a misdemeanor. They face a fine of $75,000 per property, per day in violation, more than $2 million.
Source: http://www.empirestatenews.net/News/20100114-8.html

37. *January 13, Oregonian* – (Oregon) **EPA says no to Portland's open reservoirs.** The federal government has given Portland, Oregon its final word: There is no exception to a rule requiring Portland to replace its open drinking water reservoirs. The word came in a letter to the commissioner who oversees the Water Bureau, from the assistant administrator for the U.S. Environmental Protection Agency (EPA). It appears to put an end to a long struggle between Portland and the federal agency over the rule, aimed at controlling the parasite cryptosporidium and other contaminants in drinking water. The rule also requires treatment of the city's Bull Run water supply. The city, which contends that its water supply is safe, continues to seek guidance on how to avoid building the treatment plant. The letter says the EPA found that uncovered finished water reservoirs like those in Portland "were subject to contamination from many sources including birds, animals, humans, algae, insects, and airborne deposition."

Source: http://www.oregonlive.com/portland/index.ssf/2010/01/epa_says_no_to_portlands_open.html

[Return to top]

Public Health and Healthcare Sector

38. *January 15, KIMT 3 Rochester* – (Iowa) **Firefighters respond to chemical spill at hospital.** At least one person is hurt after a chemical spill at an area medical facility. Mason City, Iowa's, fire chief says his department responded to Mercy Medical Center's West Campus at about 7:00pm Thursday night. A sodium hydroxide leak in the facilities laundry area known as Textile Services caused one person to stop breathing. He says the leak was contained to one room in the building. Crews kept people away from the spill until a private cleaning service arrived. Along with the one person hurt, four of his firefighters went to the hospital for possible exposure. They checked out in good condition.
Source: http://www.kimt.com/content/localnews/story/Firefighters-Respond-to-Chemical-Spill-at-Hospital/TQdgY7dYq0C40nlgAEqJRQ.cspx

39. *January 14, Health Data Management* – (Connecticut; National) **Health Net sued for HIPAA violations.** Connecticut's Attorney General has filed a lawsuit charging Health Net of Connecticut Inc. with violations of the HIPAA privacy and security rules following a large breach of identifiable medical records and Social Security numbers. His office believes this is the first lawsuit by a state's chief legal officer since the HITECH Act last year gave state attorneys general authority to prosecute HIPAA privacy and security violations. Parent company Health Net in Los Angeles last November reported to insurance officials in four states the disappearance in May of a hard drive with protected health information on 1.5 million members, including 446,000 in Connecticut. The data was not encrypted, but Health Net said it is invisible without the use of specific software. The company attributed the delay in reporting the breach to a lengthy forensic investigation to determine what information was on the hard drive.
Source: http://www.healthdatamanagement.com/news/breach_hipaa_privacy_security_hitech_lawsuit-39645-1.html

40. *January 14, Treasure Coast Palm* – (Florida) **Doctor's office evacuated after employee opens envelope filled with white powder.** Authorities evacuated a doctor's office after an employee opened a envelope filled with an unknown white powder Thursday afternoon. Indian River County Fire Rescue and Sheriff's deputies were called at 3:30 p.m. to the office, the fire marshal said. The envelope with the powder also contained a threatening letter. The substance will be tested to determine its contents.
Source: http://www.tcpalm.com/news/2010/jan/14/roseland-doctors-office-evacuated-after-employee/

41. *January 14, Associated Press* – (Oregon) **Ore. chemical spill sends at least 10 to hospitals.** Officials say at least 10 people went to area hospitals following a chemical spill at a health building in Oregon City. The Clackamas Fire District says emergency personnel were called to the Clackamas County Dental Clinic shortly before noon Thursday after people complained of headaches and minor respiratory symptoms. An American Medical Response spokeswoman said ambulances took 10 people to three area hospitals. Portland television station KPTV reported that the spilled chemical was formocresol, a solution used in dental work. The station says a worker dropped a jar of it. The clinic was evacuated after the spill, but reopened in the afternoon.
Source: http://www.ktvz.com/Global/story.asp?S=11825404

[Return to top]

Government Facilities Sector

42. *January 15, Associated Press* – (National) **Arkansas man pleads guilty for plotting to kill Obama.** An Arkansas man pleaded guilty Thursday to charges he plotted to kill the then-Senator and Presidential hopeful and dozens of other black people in 2008. The lead defendant, 19, of Arkansas, pleaded guilty to one count of conspiracy, one count of threatening to kill and harm a presidential candidate and one count of possessing a firearm in furtherance of a crime of violence. He faces up to 10 years in prison when he is sentenced in April. A co-defendant, 21, of Tennessee, remains in custody. Authorities have described the two as white supremacist skinheads who hatched a plot for a cross-country robbery and killing spree that was to culminate with an attack on the President, who was then a candidate for president. They were arrested in October 2008 and have been held without bond since.
Source: http://www.foxnews.com/story/0,2933,583076,00.html

43. *January 15, Denver Post* – (Colorado) **Rep. Massey reports bomb threats over medical-marijuana stance.** Three separate callers threatened to bomb a state representative's home, set it aflame and picket out front after the Poncha Springs lawmaker revealed that he would carry a medical-marijuana bill that could close dispensaries. The representative was not at home when the calls came in starting January 11. He said his wife called the Chaffee County Sheriff's Office, and surveillance has been set up at both his home and the Capitol. "My wife being there, she took it seriously," the representative said. "I would have taken it with a grain of salt." Before the governor's State of the State address, a bomb-sniffing dog checked the House chamber. The unusual security measure was a response to the threats against the representative, Capitol security said. In Poncha Springs, the Sheriff's Office put a tap on the representative's phone to identify callers, set up video surveillance and increased the frequency of patrols through his neighborhood, the sheriff said. "We take this very seriously," the sheriff said. "This medical-marijuana issue is definitely making people mad, and it involves a state representative."
Source: http://www.denverpost.com/politics/ci_14196291

44. *January 15, Pottstown Mercury* – (Pennsylvania) **Judge receives suspicious package, hazmat called in.** A Royersford, Pennsylvania man authorities allege intended to terrorize a judge's court by sending an envelope containing an unknown white powdery substance to the court was arrested for terroristic threats Thursday. The suspect was taken into police custody Thursday afternoon after a court clerk opened the letter containing the unknown substance and alerted police. The court employee immediately took precautions, not knowing whether the substance could be dangerous or toxic, the police chief said. The employee washed their hands, cleared the area where the substance was located and called police.
Source: http://www.pottsmerc.com/articles/2010/01/15/news/srv0000007333648.txt

45. *January 14, KESQ 3 Palm Springs* – (California) **Five people hospitalized after breathing toxic fumes.** Eleven people in the Hilb Student Center at College of the Desert in Palm Desert, California, reported an odor around 10:30 a.m. Thursday, and some said they were nauseated, said a spokesman for the college on Monterey Avenue. Five people were taken to a hospital for observation, while the other six refused treatment, he said. Riverside County firefighters and a Hazmat team investigated the source of the odor, said the county fire captain. Some maintenance work was being done on plumbing below the basement, and fumes from an adhesive that coats the interior of pipes to stop leaks made it through the ventilation and into the building, he said. The building will remain closed for the rest of the day, the captain said.
Source: http://www.kesq.com/Global/story.asp?S=11823562

46. *January 14, WSPA 7 Spartanburg* – (South Carolina) **"Suspicious" powder forces evacuation of attorney general's office.** A mailroom clerk working in the South Carolina attorney general's mailroom discovered a letter that had some type of powder inside Thursday morning. The letter was sent by an inmate, according a spokesman with the attorney general's office. After the powder was determined to be "suspicious", the 6th floor of the office building was evacuated by Capitol Police. The evacuation impacted about 75 people. The powder was later determined to be "non-hazardous". It was business as usual for the attorney general and the rest of his staff; no one else in the building was evacuated, but no one was allowed in or out of the building while the investigation continued.
Source:
http://www2.wspa.com/spa/news/local/article/suspiciuos_powder_forces_evacuation_of_attorney_generals_office/31917/

47. *January 13, Associated Press* – (North Dakota) **Air Force officers accused of stealing from missile launch facility allowed to resign.** Two officers accused of stealing stealing classified material from an underground missile launch facility at Minot Air Force Base in North Dakota have been allowed to resign rather than face courts-martial, the military said Wednesday. The Air Force Secretary approved the resignation of one officer in September and the second officer last month, the military said. The second officer is currently stationed at F.E. Warren Air Force Base in Cheyenne, Wyoming, and "will be out of the Air Force in the near future," an Air Force statement said. Neither suspect could immediately be reached for comment Wednesday. Neither

man had a listed telephone number, and the second officer did not immediately respond to a message left for him at the base through an Air Force spokesman. The men were missile combat crew members assigned to the base's 91st Missile Wing. They were among the crew members who work 90 feet underground prepared to launch nuclear missiles. They were accused of taking classified material in July 2005, rather than destroying it as required when it was no longer in use.
Source: http://www.latimes.com/news/nationworld/nation/wire/sns-ap-us-air-force-officers-discharge,0,3666768.story

[Return to top]

Emergency Services Sector

48. *January 15, Associated Press* – (Florida) **Officer brings strange powder, station evacuated.** A South Florida police station was evacuated after an officer brought in a suspicious white powder. The substance turned out to be cocaine. The officer, who was not named, responded late Wednesday to a home in Lighthouse Point where someone left in a mailbox a mysterious package containing white powder. In those cases, protocol is to bring in hazardous materials specialists to test the material. This time, the officer collected it and returned to the station — prompting a two-hour evacuation. He could be reprimanded, depending on the results of an internal investigation.
Source: http://www.miamiherald.com/news/florida/AP/story/1426628.html

49. *January 14, Charleston Post and Courier* – (South Carolina) **Static disrupting fire, police radio traffic.** Communications for Summerville, South Carolina, public safety are getting disrupted by static. A councilman rode with a police officer and told other council members on Monday the radio did not work well enough about 25 percent of the time "even to call in on license (checks)," he said. "It's an issue," the police chief said, but no 911 calls have been lost and no officer has been injured because of it. Asked if he was worried about either happening, he declined to comment. "It's static-y," the councilman said. "There is some problem. I don't think it impedes the police from doing their job. But we are working on improving it." Town officials are working with the vendor and the manufacturer, Motorola, to get it resolved. The problem is one more headache for police and fire officials, who have scraped along the past few years, putting off hires and hanging on to aging vehicles, as council struggled to provide for improvements while paring budgets to meet revenue shortfalls. It became an issue in the 2009 election and dominated discussions for 2009 budget cutbacks and the 2010 budget.
Source: http://www.postandcourier.com/news/2010/jan/14/static-disrupting-fire-police-radio-traffic/

50. *January 13, Hutchnews.com* – (Kansas) **911 services restored after afternoon outage.** Reno County, Kansas', 911 services were restored Wednesday afternoon after about a 2 1/2-hour outage. The outage, which occurred across south-central Kansas, was blamed on a breakdown at the AT&T 911 communication system in the Wichita Tandum Switch. At the Hutchinson/Reno County 911 Center, the assistant director said

the outage occurred at about 2:30 p.m. and covered "pretty much the entire south-central part of the state." Calls to 911 were still answered during the outage, but those who tried to call 911 in Reno County instead reached Harvey County — and vice versa — because of an agreement between the counties. Those agencies then transferred the call to the proper agency through a non-emergency line.
Source: http://www.hutchnews.com/Localregional/911--1

51. *January 13, KOAT 7 Albuquerque* – (New Mexico) **Police codes battle plain talk.** Some law enforcement agencies said that the 10-code system is too confusing while others think it is the best way to communicate. The problem with 10-code system is some local police agencies do not use the same codes as the FBI. In the past year, there has been a push to abandon the 10-code system and just use plain language. The Bernalillo, New Mexico, County Sheriff's Office said the biggest benefit of the current system is how quick it is. "We literally only have seconds when we're on a scene to make determinations of what resources we need," said a police lieutenant. According to the lieutenant, 10-82 means "need assistance" and it is quicker to use the numbers. He admitted that in an emergency with multiple agencies, they use plain talk to make sure everyone is on the same page. State police uses the 10-code system at all times, but like BCSO, if there is a large event with multiple agencies they also said they will use plain talk. APD said that they only use the 10-code system because it is quick and it is a safety issue, especially when they are around suspects. FEMA and the Department of Homeland Security are big supporters of using plain language. They came up with a manual to help agencies make the switch.
Source: http://www.koat.com/news/22232381/detail.html

[Return to top]

Information Technology Sector

52. *January 15, IDG News Service* – (International) **Conficker worm hasn't gone away, Akamai says.** Variants of the Conficker worm were still active and spreading during the third quarter, accounting for much of attack traffic on the Internet, according to Akamai Technologies. "Although mainstream and industry media coverage of the Conficker worm and its variants has dropped significantly since peaking in the second quarter, it is clear from this data that the worm (and its variants) is apparently still quite active, searching out new systems to infect," Akamai said in its State of the Internet report for the third quarter of 2009, released on January 14. During the third quarter, 78 percent of Internet attacks observed by Akamai targeted port 445, up from 68 percent during the previous quarter. Port 445, which is used by Microsoft Directory Services, is the same port that Conficker targets, aiming to exploit a buffer overflow vulnerability in Windows and infect the targeted computer. Most attacks originated from Russia and Brazil, which replaced China and the U.S., as the top two sources of attack traffic. Russia and Brazil accounted for 13 percent and 8.6 percent of attack traffic, respectively, Akamai said. The U.S., which came in at No. 3, accounted for 6.9 percent of attack traffic and No. 4 China accounted for 6.5 percent, it said.
Source:

http://www.computerworld.com/s/article/9145018/Conficker_worm_hasn_t_gone_away_Akamai_says

53. *January 15, SC Magazine* – (International) **Adobe offers conflicting statements on whether its software was connected to the Google attack.** Adobe has said in a statement that researchers have not been able to obtain any evidence to indicate that Adobe Reader or other Adobe technologies were used in the Google incident. Adobe issued a statement on January 12, saying it was aware of a computer security incident involving a sophisticated, coordinated attack against corporate network systems managed by Adobe and other companies. In an update posted on January 14, Adobe's director of product security and privacy acknowledged the 'media coverage and headlines indicating that vulnerabilities in Adobe Reader may have been the attack vector in this incident'. He said: "Just like we always do in the case of reports of security vulnerabilities in an Adobe product, we have been actively tracking down samples or other information regarding potential vulnerabilities in Adobe products related to this incident." "Similar to the McAfee researchers, we have not been able to obtain any evidence to indicate that Adobe Reader or other Adobe technologies were used as the attack vector in this incident. As far as we are aware there are no publicly known vulnerabilities in the latest versions (9.3 and 8.2) of Adobe Reader and Acrobat that we shipped on January 12, 2010. Even though we do not have any information regarding a zero-day vulnerability in an Adobe product, the sophistication of this incident also serves as a reminder to all of us the importance of layers of security to provide the best possible defense against those with malicious intent."
Source: http://www.scmagazineuk.com/adobe-offers-conflicting-statements-on-whether-its-software-was-connected-to-the-google-attack/article/161434/

54. *January 14, eWeek* – (National) **Rockefeller ready with cyber-security bill.** Prompted by Google's report that the search giant and some 20 other companies were victims of sophisticated cyber-attacks from within China, a senator promised on January 13 to mark up his cyber-security legislation early this year. Introduced by the senator and another senator from Washington in April and redrafted late this summer, the bill would create a National Cybersecurity Adviser under the authority of the president to coordinate cyber-security efforts. The two senators drafted the legislation in response to years of post-9/11 complaints that neither the private sector nor government officials were doing enough to adequately protect the nation's critical cyber-infrastructure. According to a number of reports, the senators drafted the bill after consulting with the White House. While no one particularly objected to a cyber-czar, there were howls of protest about the details in the bill. As originally drafted, the Cybersecurity Act gave the president an Internet "kill switch" for reasons of national security or in an emergency and the authority to designate private networks as critical infrastructure subject to cyber-security mandates, including standardized security software and testing, and licensing and certification of cyber-security professionals. The new language dropped all references to the president's ability to shut down the Internet. Instead, the two senators granted the president the authority to declare a cyber-security emergency and to direct the "national response to the cyber threat."

Source: http://www.eweek.com/c/a/Government-IT/Rockefeller-Ready-With-Cybersecurity-Bill-592780/

55. *January 14, eWeek* – (International) **IETF completes fix for SSL security vulnerability.** The Internet Engineering Task Force (IETF) has finished work on a fix to a vulnerability in the Secure Sockets Layer protocol security researchers uncovered last August. The vulnerability partially invalidates the SSL lock and allows attackers to compromise sites that use SSL for security — including banking sites and back-office systems that use Web services-based protocols. "The bug allows a man-in-the-middle to insert some malicious data at the beginning of a vulnerable SSL/TLS connection, but does not allow him to directly read the data sent by the legitimate parties," explained one of the individuals who found the vulnerability. "This capability is referred to as a 'blind plaintext injection attack.' Initially, it was hoped that this limited capability would offer some mitigation. Unfortunately, it seems that HTTPS is particularly strongly affected because of its design, and an effective attack on the Twitter HTTPS API was demonstrated shortly after the vulnerability was publicly disclosed." After incorporating feedback from the TLS community, the proposed fix was approved by the IESG on Jan. 7, 2010. The IESG is responsible for the technical management of IETF activities and the Internet standards process. The decision means customers can now begin to deliver patches that implement IETF's change.
Source: http://www.eweek.com/c/a/Security/IETF-Completes-Fix-for-SSL-Security-Vulnerability-589986/

56. *January 14, Computerworld* – (International) **Microsoft confirms IE zero-day behind Google attack.** Microsoft issued a security advisory Thursday that warned users of a critical and unpatched vulnerability in Internet Explorer (IE), and acknowledged that it had been used to hack several companies' networks. "We have determined that Internet Explorer was one of the vectors used in targeted and sophisticated attacks against Google and possibly other corporate networks," said the director of Microsoft's Security Response Center (MSRC), in a post to the group's blog. Earlier on January 14, antivirus company McAfee said the IE bug had been exploited by hackers who had attacked computer networks of nearly three dozen major companies between mid-December 2009 and January 4, 2010. McAfee said then that Microsoft would soon release this advisory. The security advisory said that the only version of IE not containing the critical flaw was IE 5.01 running on Windows 2000. All other versions, including IE6, IE7 and IE8 on Windows 2000, XP, Server 2003, Vista, Server 2008, Windows 7 and Server 2008 R2 are vulnerable to attack. Even so, the director downplayed the threat to average Windows users.
Source:
http://www.computerworld.com/s/article/9144938/Microsoft_confirms_IE_zero_day_behind_Google_attack

57. *January 14, Washington Post* – (National) **Google China cyberattack part of vast espionage campaign, experts say.** Computer attacks on Google that the search giant said originated in China were part of a concerted political and corporate espionage effort that exploited security flaws in e-mail attachments to sneak into the networks of

major financial, defense and technology companies and research institutions in the United States, security experts said. At least 34 companies — including Yahoo, Symantec, Adobe, Northrop Grumman, and Dow Chemical — were attacked, according to congressional and industry sources. Google, which disclosed on January 12 that hackers had penetrated the Gmail accounts of Chinese human rights advocates in the United States, Europe, and China, threatened to shutter its operations in the country as a result. Human rights groups as well as Washington-based think tanks that have helped shape the debate in Congress about China were also hit. Security experts say the attacks showed a new level of sophistication, exploiting multiple flaws in different software programs and underscoring what senior administration officials have said over the past year is an increasingly serious cyber threat to the nation's critical industries. "Usually it's a group using one type of malicious code per target," said the head of international cyber-intelligence for VeriSign's iDefense Labs, a Silicon Valley company helping some firms investigate the attacks. "In this case, they're using multiple types against multiple targets — but all in the same attack campaign. That is a marked leap in coordination."
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

58. *January 13, Network World* – (International) **DDoS attacks are back (and bigger than before).** Distributed denial-of-service (DDoS) attacks are not new. Companies have suffered the scourge since the beginning of the digital age. But DDoS seems to be finding its way back into headlines in the past six months, in thanks to some high-profile targets and, experts say, two important changes in the nature of the attacks. The targets are basically the same — private companies and government websites. The motive is typically something like extortion or to disrupt the operations of a competing company or an unpopular government. But the ferocity and depth of the attacks have snowballed, thanks in large part to the proliferation of botnets and a shift from targeting ISP connections to aiming legitimate-looking requests at servers themselves. In fact, said the CSO of Cambridge, Massachusetts-based Akamai Technologies, the botnets launching many of today's DDoS attacks are so vast that those controlling them probably lost track of how many hijacked machines they control a long time ago. "We see a lot less of the fire-and-forget malware-based attacks designed to bog down the machines that were infected," the CSO said, referring to old-school worm attacks like Blaster, Mydoom, and Code Red. "Now the malware is used to hijack machines for botnets and the botnets themselves are used as the weapon."
Source: http://www.networkworld.com/news/2010/011410-ddos-attacks-are-back-and.html?hpg1=bn

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

59. *January 15, Brown News Service* – (Ohio) **Damaged line knocks out phone service.** A damaged fiber optic line in Brown County caused interruption to 911 service, cellular phones and long distance service in Adams and Brown counties for about five hours on January 11. Although the line directly affected Verizon customers, AT&T cellular customers were also out of service. Verizon, who is in the process of selling their Ohio land lines to Frontier Communications, said the aerial line was damaged on Hamer Road, south of Sardinia and Tracy Road in Brown County, at about 3:30 p.m. In addition to disrupting land line service, the fiber optic line also feeds a nearby cell phone tower that was temporarily disrupted as a result. "The fiber line was damaged by someone, however we do not believe it was vandalism," the manager of North Central Media Relations for Verizon said on January 12. "We had everything transferred to the Highland County Sheriff's Office, the Adams County Sheriff's Office and to our regular business line," said the Adams County 911 director.
Source:
http://www.peoplesdefender.com/main.asp?SectionID=13&SubSectionID=83&ArticleID=130861

60. *January 14, Dallas Morning News* – (Texas) **ATT doesn't know what caused 3G network outage.** AT&T Inc. said its cellular network in the Dallas area suffered from an unexplained outage on January 14. Several AT&T customers reported that the problems ceased when they turned off access to 3G on their phones and resorted to the slower 2G network. Critics have complained recently that AT&T's network in many cities is buckling under the strain of so many new 3G users, particularly iPhone users. While AT&T acknowledged network problems in New York and San Francisco, it has said its service elsewhere has performed well despite the influx of 3G devices. The Dallas-based company said it was working to restore service.
Source:
http://www.dallasnews.com/sharedcontent/dws/bus/industries/techtelecom/stories/011509dnbusattoutage.7b7f3623.html

61. *January 14, Newton Kansan* – (Kansas) **Phone line outage cuts Harvey County 911 service.** Emergency calls to 911 had to be rerouted Wednesday after a cut communications cable resulted in a service interruption that affected several south-central Kansas counties. Service went down about 1:30 p.m. in Harvey County and was down for about three hours, until 4:30 p.m., said the assistant director of Harvey County Communications. The loss of service meant calls did not go through between cities or between the 316 and 620 area codes. The cities of Burrton, Hesston, and Walton set up answering points to redirect emergency calls. Calls in Newton, Halstead, Sedgwick, and Whitewater were redirected to local numbers. Harvey County's back-up is in Hutchinson, which also was affected by the outage. The assistant director said he thought Sumner and Butler counties also were affected. The assistant director said there was one Hesston EMS call that had to be rerouted, but the reporting party used a cell

phone and was able to get through to emergency personnel.
Source: http://www.thekansan.com/topstories/x1672010202/Phone-line-outage-cuts-Harvey-County-911-service

For more stories, see items **49** and **50**

[Return to top]

Commercial Facilities Sector

62. *January 15, Tribeca Trib* – (New York) **Fire forces many to evacuate Lower Manhattan office tower.** The acrid smell of smoke hung in the air inside the lobby of a lower Broadway office tower Thursday night, after a fire on the second floor forced dozens of workers out of the building. As many as 30 fire trucks and ambulances responded to the fire at 45 Broadway, a 32-story office building just a few blocks from the World Trade Center site. The fire apparently started inside an exterior second-floor overhang around 6:15 p.m., January 14, and quickly filled the lower floors of the tower with smoke. A spokesman for the city's Fire Department said no one had been injured or hospitalized as a result of the fire. It took just over an hour to quell the blaze, the exact cause of which has not been determined. One building occupant said crews had been working in the overhanging portion of the structure where it started earlier in the day, apparently repairing a problem with his heating and air conditioning. A Fire Department spokesman said only the tower's lower floors were evacuated during the fire, but reports from inside the building indicate that all workers were eventually told to evacuate their offices.
Source: http://www.tribecatrib.com/news/2010/january/477_fire-forces-many-to-evacuate-lower-manhattan-office-tower.html

63. *January 14, KOVR 13 Sacramento* – (California) **OC building evacuated, man smears blood on walls.** Police say a three-hour search turned up no sign of a man who broke windows with a baseball bat in a high-rise building in Orange County, California, and smeared blood on the walls. The building in the city of Orange was evacuated after the man set off fire alarms and told people the building was on fire Thursday morning. An Orange police sergeant says officers and dogs searched the building floor-by-floor, but could not find the man. Investigators are also interviewing witnesses and reviewing security camera footage. He says the building houses offices belonging to attorneys and investment companies. Witnesses say the man looked like he was bleeding. No other injuries were reported.
Source: http://cbs13.com/wireapnewsca/Police.evacuate.high.2.1426801.html

64. *January 14, Associated Press* – (Alaska) **Bomb donated to Kodiak museum goes out with a bang.** A World War II relic that was displayed outside an Alaska bar for years turned out not to be a dud. Soldiers on Wednesday detonated the 1,263-pound aerial bomb. Radio station KMXT reports it lost some of its boom after 60 years, but it did go with a bang. The ordnance was recently donated to the Kodiak Military History Museum by a local resident, but the museum director determined it was more than just

an interesting artifact. Soldiers from the Fort Richardson Explosive Ordnance detail inspected the bomb and determined it still had Dunnite, a highly explosive material also known as "Explosive D." They recorded the detonation and salvaged a piece of the bomb for display at the museum.
Source: http://www.msnbc.msn.com/id/34868834/ns/us_news/

65. *January 14, Globe and Mail* – (International) **U.S. notes Al Qaeda Olympic threat.** The U.S. government is advising American sports fans traveling to Vancouver for the 2010 Winter Olympics to watch out for Al-Qaeda and other extremists, especially on transit and in restaurants, churches and other areas outside official venues. "Al-Qaeda's demonstrated capability to carry out sophisticated attacks against sizable structures — such as ships, large office buildings, embassies and hotels — makes it one of the greatest potential threats to the Olympics," the U.S. State Department said in a fact sheet on the Games posted on its website. No specific credible threats have been identified, the U.S. government said. However, Americans planning to attend Olympic events or participate in large-scale public gatherings during the Winter Games should use caution and be alert to their surroundings, the advisory said. Americans are advised to be especially alert when outside Olympic venues. "As security increases in and around Olympic venues, terrorists could shift their focus to more unprotected Olympic venues, open spaces, hotels, railway and other transportation systems, churches, restaurants, and other sites not associated with the Olympics."
Source: http://www.ctvolympics.ca/about-vancouver/news/newsid=25959.html

[Return to top]

National Monuments and Icons Sector

66. *January 14, KESQ 3 Palm Springs* – (California) **Fire erupts at Lake Elsinore.** A roughly 30-acre brush fire broke out Thursday in a remote area of the Cleveland National Forest along Ortega Highway, west of Lake Elsinore in California, a Forest Service spokesman said. The fire was reported just after noon, about 5 miles west of Lake Elsinore, close to the Riverside/Orange county line, said a forest service information officer. The blaze is being battled from the air as well as the ground.
Source: http://www.kesq.com/Global/story.asp?S=11824572

67. *January 14, Idaho Statesman* – (Idaho) **Forest Service will spend more money to manage beetles in Idaho, Minnick says.** The U.S. Agriculture Secretary agreed to spend an additional $14 million to combat bark beetles in Idaho forests. An Idaho U.S. Representative announced the funding in Nampa Thursday. "This issue has been one of my most important since taking office," said the Representative, a former forest products industry executive. "Bark beetles are a huge menace to our forests, and throughout Idaho you can see the irreparable damage they are doing as dead and dying trees litter the mountainside," said the ranking member of the Interior and Environment Appropriations Subcommittee.
Source: http://www.idahostatesman.com/environment/story/1041710.html

68. *January 14, Associated Press* – (Arizona) **Arizona may shut down two-thirds of state parks.** Arizona is on the verge of permanently closing more than half of its state parks to ease its budget woes — the most drastic such proposal in the nation and one that could mean shutting down some iconic Old West locations. The plan would close the Tombstone Courthouse and the Yuma Territorial Prison, and shut down parks that draw tens of thousands of tourists a year such as Red Rock State Park in Sedona. "We don't have a choice. It's either shut them all down right now or shut them down in phases, and we're picking the ones that cost the state money," said the head of the Arizona Parks Board, which plans to take up a staff recommendation to close 13 parks by June 3. State officials closed five parks last year. If the additional closures are approved, two-thirds of the state parks in Arizona will be shut down. Arizona is not the only place where lawmakers are targeting parks, but it is taking the most aggressive action, said the executive director of the National Association of State Parks Directors. California's governor last year proposed closing 220 of California's 279 parks in the face of a multibillion-dollar deficit. But the governor backed off four months later after protests from park activists.
Source: http://abcnews.go.com/Business/wireStory?id=9565125

[Return to top]

Dams Sector

69. *January 14, Enquirer* – (Kentucky; Indiana) **Markland Dam repairs continue.** Two gates from the closed main lock chamber at Markland Locks and Dam will be shipped back upriver Monday after undergoing repairs in Louisville, Kentucky. The Army Corps of Engineers expects the 1,200-foot lock will reopen to river traffic in March. "With the help from other Army Corps of Engineers districts, we've repaired the damaged lock gate leaves, and now four to five more weeks of work remain in order to reopen the 1,200-foot lock," the commander of the Corps of Engineers' Louisville District said in a news release. "If the river continues to run low we plan to finish the work, re-hang the gates and return the lock chamber to service by March 1." The lock has been closed since one of the 250-ton miter gate leaves failed and plunged into the water September 27. River traffic has been forced to pass through the dam's smaller auxiliary lock since.
Source:
http://nky.cincinnati.com/apps/pbcs.dll/article?AID=/AB/20100114/NEWS0103/301140018

70. *January 13, KMVT 11 Twin Falls* – (Idaho) **Proposed changes to Minidoka Dam.** Over a century of use is taking a toll on the Minidoka Dam in Idaho. Officials say, over 2,000 feet of spillway has reached functional limit. Concrete forms are suffering deterioration. Bureau of Reclamation officials say it is time for some maintenance and time for some public input. The activity manager said, "The draft presents and evaluates proposed alternatives for correcting structural problems within the spillway and irrigation canal headworks — both structures are showing quite a bit of decay." Officials are exploring three options in fixing the dam's growing problems.

She said, “In addition to the no action alternative — which is leaving the structure currently as it is, with continuing operation and maintenance, we’re looking at other alternatives.” Alternative B is to replace both the spillway and the headworks. Alternative C is looking at replacing just the spillway. But bureau officials say if they are going to do repairs, they want to go all the way, replace both the spillway and the headworks.
Source: http://www.kmvt.com/news/local/81349692.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

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