Daily Open Source Infrastructure Report
25 January 2012

Top Stories

- A burst of radiation on the sun's surface triggered a geomagnetic storm on Earth January 24 that caused rerouting of flight routes, may have disrupted satellite communications and the Global Positioning System. – *San Francisco Chronicle* (See item **31**)
- A researcher located and mapped more than 10,000 industrial control systems hooked up to the public Internet, and found many were open to easy hack attacks because of lax security. – *Wired* (See item **37**)

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 24, Rochester Democrat and Chronicle* – (New York) **RG&E, NYSEG disclose security breach.** The New York Public Service Commission is investigating unauthorized access to the personal information of Rochester Gas and Electric Corp. (RG&E) and New York State Electric and Gas Corp. (NYSEG) customers — including

Social Security numbers, dates of birth, and some financial institution account data. The Rochester-based companies said January 23 that an employee at a software consulting firm contracted by RG&E and NYSEG allowed the access to one of the companies' customer data systems. The utilities said there is no evidence any customer data have been misused, and that there is no indication of malicious intent. Law enforcement authorities have been contacted, the companies said, and an internal investigation is under way. The state's investigation will focus on the company's plans to identify, communicate with, and help affected customers. It will also look for the root causes of the security breach, and what measures are in place to protect customer information.
Source: http://www.democratandchronicle.com/article/20120124/NEWS01/201240330

2. *January 24, WABC 7 New York* – (New Jersey) **Deadly NJ tanker crash sends fireball into the sky.** A gasoline tanker exploded in a collision with a car in Elizabeth, New Jersey, killing one person and closing Routes 1 and 9 while sending a fireball into the sky January 24. The car and tanker crashed at the intersection of Bayway Avenue just before 1:45 a.m. The vehicle became wedged under the burning tanker, trapping the driver by the fireball. The driver of the car was pronounced dead at the scene. The driver of the tanker escaped his burning truck without serious injury. Firefighters closed off the busy Bayway Circle, a main route to the Goethals Bridge, as they battled the flames with foam trucks. Authorities were expected to be on the scene for hours.
Source:
http://abclocal.go.com/wabc/story?section=news/local/new_jersey&id=8516502

3. *January 23, Enid News and Eagle* – (Oklahoma) **Investigation of oil well blast ongoing.** The Oklahoma Corporation Commission is investigating an oil well explosion and fire that occurred January 20 in Logan County, Oklahoma. Four workers were injured in the blast at a Kirkpatrick Oil Co. well located about 2 miles north of the intersection of Oklahoma 51 and Oklahoma 74. A spokesman for the commission said it is too early to make a ruling on the cause. He said preliminary indications show no environmental damage was done and safety issues will be investigated by the Occupational Safety and Health Administration. El Dorado Drilling Co., an affiliate of Kirkpatrick Oil Co., operates the rig. El Dorado provides contract drilling services in northwest and north central Oklahoma for independent oil and gas production companies, according to the El Dorado Web site.
Source: http://enidnews.com/localnews/x1296866301/Investigation-of-oil-well-blast-ongoing

4. *January 23, Associated Press* – (Oklahoma) **Authorities probe explosions at Okla. business.** The FBI and local law enforcement agencies are investigating a series of explosions at a gas and propane business in Stilwell, Oklahoma. An FBI special agent said authorities received emergency calls between 3 a.m. and 4 a.m. January 23 that three separate blasts had occurred at the Anderson Gas and Propane Co. The FBI agent said investigators believe the explosions were intentionally set. There have been no reports of injuries, and damage to the business was minor. The agent could not confirm what types of devices were used. The Bureau of Alcohol, Tobacco, Firearms, and Explosives, the Oklahoma Highway Patrol, Stilwell police, and the Adair County

Sheriff's office were also investigating.
Source: http://www.newson6.com/story/16582530/authorities-probe-explosions-at-okla-business

For more stories, see items **5**, **31**, **37**, and **40**

[Return to top]

Chemical Industry Sector

See item **37**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

5. *January 24, Minot Daily News* – (North Dakota) **Officials to test Minot proppant after oilfield waste found radioactive.** The North Dakota Department of Health said January 23 it will be testing bags filled with proppant sand stacked in Minot for radioactivity. The decision stems from recent news the Williston landfill rejected 23 loads of oilfield waste since June due to radioactive contamination. An independent testing firm called in to investigate the situation found ceramic proppant, as well as filter socks used in the process of preparing "frack sand" to be pumped into the ground, to be radioactive. The materials found were determined to be naturally occurring radioactive materials, but the quantities of the materials turning up in testing is far above the levels found in nature. Those materials were traced to proppant originating in China, according to the director of the North Dakota Department of Health's Air Quality Division.
Source: http://www.minotdailynews.com/page/content.detail/id/562393/Officials-to-test-Minot-proppant-after-oilfield-waste-found-radioactive.html?nav=5010

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

[Return to top]

Critical Manufacturing Sector

See items **37** and **41**

[Return to top]

Defense Industrial Base Sector

See item **37**

[Return to top]

Banking and Finance Sector

6. *January 24, Charlotte Observer* – (North Carolina) **6 charged in Charlotte-area mortgage scheme.** Federal prosecutors filed charges against six Charlotte, North Carolina-area defendants over mortgage fraud-related offenses and a "builder kickback" scheme, the latest fallout from the housing market bust, the Charlotte Observer reported January 24. The defendants are accused of working with Charlotte home builder Tara Properties to sell houses by offering kickbacks to straw buyers. The kickbacks were not disclosed to lenders or included on loan applications, according to documents filed last week in federal court. The scheme resulted in hundreds of sales between January 2005 and February 2008, with Tara paying more than $5 million in kickbacks, the filings say. The conspirators fraudulently caused lenders to provide more than $42 million in loans, prosecutors allege. Tara specialized in building homes priced between $100,000 and $200,000 and the company offered kickbacks of 15 percent of the sales price. Defendants lied on loan applications about income and assets, employment, debts, and anticipated debts, and intent to occupy the home as a primary residence, court documents say. Some applications also contained false or forged documents such as bogus payroll stubs and bank statements. The straw buyers recruited by the promoters and mortgage brokers generally were unqualified to obtain the loans, and the "vast majority" of homes lapsed into foreclosure, according to prosecutors. The six defendants indicted the week of January 16 in connection with the builder-kickback scheme have been charged with mortgage fraud conspiracy, and money laundering conspiracy.
   Source: http://www.wcnc.com/news/local/6-charged-in-Charlotte-area-mortgage-scheme-137949413.html

7. *January 23, Birmingham Business Journal* – (Alabama) **Wells Fargo, Regions branches among businesses damaged in Center Point.** Banks and several other businesses in Center Point, Alabama, were damaged by storms that swept through Jefferson County January 23. The Wells Fargo and BBVA Compass branches on Center Point Parkway were heavily damaged and were closed the morning of January 23. Representatives from Wells Fargo said the downtown branch would open at 10:30 a.m. A spokesperson from BBVA Compass said the bank sustained only minor damage and was expected to reopen January 24. Regions Bank 's Center Point branch was also closed due to minor damage. Regions' Deerfoot Parkway and Pinson branch locations were closed due to road and power issues in those areas. A Regions representative said there were power outages in market areas outside of Birmingham that have been impacted by the severe weather, and that isolated branch closings would be possible.
   Source: http://www.bizjournals.com/birmingham/news/2012/01/23/wells-fargo-branch-other-businesses.html

8. *January 23, U.S. Department of Treasury* – (International) **Treasury designates major Iranian state-owned bank.** The U.S. Department of the Treasury January 23 designated Iran's third-largest bank, Bank Tejarat, for providing financial services to several Iranian banks and firms already subject to international sanctions for involvement in Iran's weapons of mass destruction (WMD) proliferation activities. With the January 23 action, 23 Iranian-linked financial institutions, including all of

Iran's largest state-owned banks, have been sanctioned by the United States based on their involvement in Iran's illicit activities. Bank Tejarat was designated pursuant to Executive Order (E.O.) 13382 (Blocking Property of WMD Proliferators and Their Supporters) for providing financial services to Bank Mellat, the Export Development Bank of Iran (EDBI), the Islamic Republic of Iran Shipping Lines (IRISL), and the Ministry of Defense for Armed Forces Logistics (MODAFL), all of which were previously designated by Treasury or the Department of State for involvement in Iran's WMD proliferation activities. Trade Capital Bank also was designated January 23 for providing financial services to EDBI, and for being owned or controlled by Bank Tejarat. Bank Tejarat has nearly 2,000 branches throughout Iran, as well as foreign branches in France and Tajikistan. Trade Capital Bank is a Belarus-based bank owned by Bank Tejarat. Bank Tejarat has directly facilitated Iran's illicit nuclear efforts. For example, in 2011, Bank Tejarat facilitated the movement of tens-of-millions of dollars in an effort to assist the Atomic Energy Organization of Iran's ongoing effort to acquire uranium.
Source: http://www.treasury.gov/press-center/press-releases/Pages/tg1397.aspx

9. *January 23, WCMH 4 Dublin* – (Arizona; Ohio) **2 plead guilty to $15 million mortgage fraud scheme.** Two central Ohio men pleaded guilty in connection with a $15 million mortgage fraud scheme that cost lenders more than $6 million, WCMH 4 Columbus reported January 23. The men pleaded guilty to fraudulently obtaining about $15 million in mortgage loans to finance the purchase of 26 real estate properties in Maricopa County, Arizona. The guilty pleas were entered January 17 and January 20. Officials said that between August 2006 and May 2007, the two men applied for loans using false income, assets, and occupancy statements on the applications. The loans were inflated to allow the man to use the excess mortgage proceeds to generate cash kickbacks payable to co-conspirators that were undisclosed to the lenders. The co-conspirators then provided the money to the men via interstate wire transfers, investigators said. They said the men used a mortgage brokerage company they co-owned, Vanguard Mortgage, in Westerville, to finance the purchases of the properties. Each man inflated his income, minimized his assets, failed to disclose his ownership of several other properties on which he held loans, and concealed the fact he intended to receive substantial cash kickbacks after the closing of three properties. All 26 of the Arizona properties were subsequently sold short or foreclosed upon due to borrowers being unable to pay the monthly payments. Each man pleaded guilty to one count of money laundering, which is punishable by up to 10 years in prison, a fine of up to $250,000 or twice the value of the property involved, whichever is greater, and restitution to the victims.
Source: http://www2.nbc4i.com/news/2012/jan/23/two-plead-guilty-15-million-mortgage-fraud-scheme-ar-907064/

10. *January 23, Kansas City Business Journal* – (International) **Euronet faces first criminal computer breach of secure payment data.** Euronet Worldwide Inc., a Leawood, Kansas company that provides secure payment services, has reported a criminal computer security breach. Euronet said the breach targeted a "small portion" of its European business in late 2011, according to a January 23 filing with the Securities and Exchange Commission. The event marks the global electronic payments

provider's first data breach, the company's chief executive officer (CEO) said. "(We), like hundreds of thousands of other companies, have been hacked into, but we were able to find it early, plug the hole ... and our breach has been contained for well over a month," the CEO said. He said the breach affected card data in Euronet's electronic fund transfer division, a European unit that makes up 17 percent of its business. Third-party forensic investigators confirmed the breach did not affect Euronet's other business units, including its epay division, ATM networks, or money-transfer operations, the company reported in the filing. The CEO said that of the electronic fund transfer division, 90 percent of the data on card transactions remained protected. He partially credited a highly secure microchip that appears on most European debit and credit cards. The chip requires a verification PIN for access. The 10 percent of data that became exposed stemmed from older cards that had not yet been updated with the chip, he said.
Source: http://www.bizjournals.com/kansascity/news/2012/01/23/euronet-faces-first-criminal-computer.html?page=all

11. *January 23, Sacramento Bee* – (California) **Three Sacramento women arrested in false tax return scheme.** Three Sacramento, California women were arrested January 23, accused of stealing taxpayers' identities and their tax refunds. According to federal court documents, the women have been charged in a conspiracy to defraud the United States through the filing of false tax returns using TurboTax, an income tax preparation software and filing service. The women are charged with executing a mail fraud scheme to obtain Green Dot debit cards, a service offered through the TurboTax software, loaded with the tax return money of taxpayer victims. In addition to the conspiracy, one of the women is charged with 15 counts of filing false tax returns, 20 counts of mail fraud, and eight counts of aggravated identity theft. Another is charged with five counts of filing false tax returns, 15 counts of mail fraud, and one count of aggravated identity theft, according to a federal Department of Justice news release. The alleged fraudulent tax return claims filed by the three women amount to more than $1,366,427, with an actual paid Internal Revenue Service (IRS) loss of about $962,079. The scheme involved more than 280 false tax returns and numerous victim taxpayers, officials said.
Source: http://blogs.sacbee.com/crime/archives/2012/01/three-sacramento-women-arrested-in-false-tax-return-scheme.html

12. *January 23, Computerworld Australia* – (International) **Researcher traces 'Gameover' malware to maker of Zeus.** The "Gameover" malware that the FBI warned users about earlier in January 2012 is a preview of the next version of the even-more-notorious Zeus money-stealing trojan, a security researcher said January 23. "Gameover represents the latest and greatest source code package from the Zeus author," a senior security researcher with Dell SecureWorks' counter-threat unit said. "[New features] in Gameover will be rolled into the final Zeus version 3, which is in beta and will wrap up soon if it hasn't already." Two weeks ago, the FBI warned of increased action by Gameover, including rounds of spam that tried to dupe recipients into infecting their PCs with the malware, which like Zeus, is designed to pillage individuals' and companies' bank accounts. The security researcher, who has been tracking the Zeus malware and its developer for years, said Gameover posed a new and

more dangerous threat because it had been created by the maker of Zeus specifically at the behest of one of his biggest clients. "The crew using Gameover has requested a lot of changes in the Zeus functionality," he said, adding the hacker crew using Gameover has direct access to Zeus' maker because it pays him well and often for support. "The Zeus author now has only three or four major clients," he said. The criminal coder abandoned all his "small fish" to focus on supporting a handful of customers who pay top dollar for his work. The additions demanded by the Gameover gang, which the Zeus developer quickly created, included a new, more distributed form of command-and-control (C&C) that uses a peer-to-peer function to update infected machines when or if a botnet's single C&C server is discovered by authorities and taken offline. Gameover also supports the use of complex Web injections that allow criminals to bypass multi-factor authentication now used by many financial institutions to stymie account plundering. And the crew apparently asked for changes to Zeus that would let the gang rent third-party botnets that specialize in conducting distributed denial-of-service (DDoS) attacks, the researcher added.
Source:
http://www.computerworld.com/s/article/9223642/Researcher_traces_Gameover_malware_to_maker_of_Zeus?taxonomyId=17

For more stories, see items **40** and **47**

[Return to top]

Transportation Sector

13. *January 24, Fox News* – (International) **Delta reroutes planes following massive solar eruption.** An immense blast of plasma spewed from the sun January 22, led to the strongest radiation storm bombarding our planet since 2005 — and even forced Delta Air Lines to redirect certain high-flying airplanes. National Oceanic and Atmospheric Administration's (NOAA) Space Weather Prediction Center — the nation's official source of warnings about space weather and its impact on Earth — issued a watch for a geomagnetic storm that begun to hit January 24 after a satellite witnessed an ultraviolet flash from the massive solar eruption. There is no risk to people on Earth, a spokesman of the NOAA Space Weather Prediction Center told FoxNews.com. But as a rare precaution, some polar flights were re-routed to avoid exposing pilots and passengers to excessive radiation. Delta is rerouting flights between Hong Kong and the United States that usually fly over the pole. The changes — mainly intended to prevent loss of radio communication — affected about six flights January 24; the airline will re-evaluate January 25 to determine whether additional changes will be required.
Source: http://www.foxnews.com/scitech/2012/01/23/planes-rerouted-fearing-strongest-radiation-storm-in-7-years/#ixzz1kO1FpLST

14. *January 24, KJRH 2 Tulsa* – (Oklahoma) **12 train cars derail, close highway in Rogers County.** A series of train cars that derailed overnight in Inola, Oklahoma has shut down State Highway 88 for most of the morning, January 24. Union Pacific said 12 cars carrying a mixed load of coal, scrap metal, and flour derailed around midnight,

just south of 412. The rail company brought in equipment from Tulsa and Kansas to clear the area. Rogers County sheriff's deputies said the derailment did not affect homes or businesses. At around 10:30 a.m. crew reopened one lane of Highway 88. The track speed is 49 miles-per-hour. Investigators were working to determine if speed was a factor in the accident.
Source: http://www.kjrh.com/dpp/news/state/12-train-cars-derail-close-highway-in-rogers-county

15. *January 24, Californian.com* – (California) **Storm damage closes Highway 1 in Big Sur.** A rainstorm caused a rockslide January 22 at a bridge construction site on Highway 1 in Big Sur, California, 50 miles south of Carmel, shutting down the highway, and forcing motorists to turn back. On January 24, Big Sur and coastal businesses remained open. The slide, which came down a steep, slide-prone cliff and spilled out from underneath mesh safety netting, blocked half the roadway. California Department of Transportation (Caltrans) crews were assessing the situation for the best way to proceed, said a Caltrans spokesman from District 5 headquarters in San Luis Obispo. Caltrans personnel at the scene said the highway would be closed overnight and probably reopen sometime January 24. To improve safety, a bridge was built at the slide site to move traffic away from the cliff, and a "slide shed" was being installed to keep rocks from striking vehicles, the spokesman said.
Source: http://www.thecalifornian.com/article/20120124/NEWS01/201240310/Storm-damage-closes-Highway-1-Big-Sur?odyssey=nav|head

16. *January 23, Next Gov* – (National) **Hackers manipulated railway computers, TSA memo says.** Hackers, possibly from abroad, executed an attack on a Northwest rail company's computers that disrupted railway signals for 2 days in December, according to a government memo recapping outreach with the transportation sector during the emergency. On December 1, train service on the unnamed railroad "was slowed for a short while" and rail schedules were delayed about 15 minutes after the interference, stated a Transportation Security Administration (TSA) summary of a December 20 meeting about the episode obtained by Nextgov. The following day, shortly before rush hour, a "second event occurred" that did not affect schedules, TSA officials added. On January 23, officials at the DHS said that following additional in-depth analysis, it appears the rail infiltration may not have been a targeted attack. "On December 1, a Pacific Northwest transportation entity reported that a potential cyber incident could affect train service," a DHS spokesman said. "The Department of Homeland Security, the FBI, and our federal partners remained in communication with representatives from the transportation entity in support of their mitigation activities and with state and local government officials to send alerts to notify the transportation community of the anomalous activity as it was occurring."
Source: http://www.nextgov.com/nextgov/ng_20120123_3491.php

For more stories, see items **2**, **31**, **37**, **47**, **48**, and **49**

[Return to top]

Postal and Shipping Sector

17. *January 24, Associated Press* – (Georgia) **39,000 pounds of junk mail bound for Florida burns on highway.** Authorities said they determined nearly 39,000 pounds of mail bound for Florida burned on the side of a Georgia highway in Waycross, the Associated Press reported January 24. A U.S. Postal Service spokesman told the Florida Times-Union that all 38,616 pounds was advertising mail, also known as junk mail. The Waycross postmaster determined there was no first-class mail among the cargo of the burned-out semitrailer. Authorities said a truck driver saw flames coming from around the rear wheels of his semitrailer January 21. Firefighters extinguished the fire, but the mail had already burned.
Source: http://www.myfoxorlando.com/dpp/news/state_news/012412-junk-mail-bound-for-florida-burns-on-highway

[Return to top]

Agriculture and Food Sector

18. *January 24, RTTNews* – (National) **Jones' Seasoning recalls products over possible Salmonella contamination.** Jones' Seasoning Blends LLC is voluntarily recalling its products — Jones' Mock Salt Original and Jones' Mock Salt Spicy Southwest Blend on possible contamination of Salmonella, RTTNews reported January 24. Jones' Mock Salt Original and Jones' Mock Salt Spicy Southwest Blend are seasoning products containing organic garlic, organic onion, organic celery seeds, organic black pepper, and organic orange peel as some of the ingredients. Salmonella contamination of the celery seeds ingredient used in Jones Mock Salt is the cause for the recall of the products. Jones Seasoning Blends LLC said that it is not responsible for the Salmonella contamination, and that the supplier of the celery seeds has been recalling the product. The affected products were directly distributed to grocery stores and markets in California, Minnesota, and Washington as well as sold through Internet orders.
Source:
http://www.rttnews.com/Story.aspx?type=bs&Id=1803506&Category=FDARecall

19. *January 23, Five Towns Patch* – (New York) **15 treated for carbon monoxide inhalation in North Lawrence.** Fifteen people were treated by local fire departments for carbon monoxide inhalation January 23 in Lawrence, New York, after a leak was discovered at a commercial food shipping company, according to the chief of the Lawrence-Cedarhurst Fire Department (LCFD). A call came in to the department about people feeling nauseous and experiencing headaches at Commodity Forwarders, the chief said. Members of the LCFD evacuated the building and donned protective equipment. They found extreme levels of carbon monoxide in the building and called the Nassau County Hazardous Materials Unit to assist. Seven people were sent to the hospital for further treatment. The source of the leak was determined to be a faulty forklift, which caused the gas to build up in the building. The building was ventilated with high-pressure fans.

Source: http://fivetowns.patch.com/articles/14-treated-for-carbon-monoxide-inhalation-in-north-lawrence

20. *January 23, Minneapolis Star Tribune* – (Wisconsin) **Feds fault Hormel on safety violations.** Federal workplace safety regulators cited a Hormel Foods subsidiary January 23 for rare "willful" safety law violations in connection with an accident in the summer of 2011 that severed a turkey plant worker's arm. The man, a veteran employee, was cleaning equipment July 20 at a Jennie-O Turkey Store processing plant in Barron, Wisconsin, when his arm became snared in a moving production line. The arm was reattached after he was flown to a hospital. Jennie-O should not have allowed cleaning of any sort while the production line was running, said a spokeswoman for the Occupational Safety and Health Administration (OSHA). The agency has proposed fines of $318,000. Jennie-O, which employs 1,200 at its Barron plant, is one of the nation's largest turkey processors. The OSHA issued 11 citations to Jennie-O, seven of them deemed "serious" and four "willful."
Source: http://www.startribune.com/business/137934633.html

For another story, see item **37**

[Return to top]

Water Sector

21. *January 24, Minot Daily News* – (North Dakota) **Authorities investigate water tower vandalism.** Authorities are investigating a case of vandalism at a $1.8 million water tower south of Minot, North Dakota, the Minot Daily News reported January 24. While testing was being performed on the 750,000-gallon water tower January 9, workers discovered the tank was riddled with holes. Photos show that about a dozen holes were shot with a rifle into the top of the tower and so far there are no tips on who the perpetrator was. A reward of up to $25,000 has been made available. The water tower, which serves residents in the Parshall and White Shield communities on the Fort Berthold Reservation, is fairly new. It is usable, "but we're going to lose water out of it every time we fill it up," officials said. The tower will be temporarily fixed as final repair work cannot be completed during the winter months.
Source: http://www.minotdailynews.com/page/content.detail/id/562387/Authorities-investigate-water-tower-vandalism.html?nav=5010

22. *January 24, WPTV 5 West Palm Beach* – (Florida) **Explosion at solid waste authority plant in West Palm Beach sends one person to the hospital.** One person was injured after an explosion at the Solid Waste Authority plant in West Palm Beach, Florida, January 24, according to a Palm Beach County Fire Rescue spokesperson. Crews responded to the scene shortly before 6 a.m. The explosion happened at 5:31 a.m. at the authority's bio solids processing facility. The injured person was taken to the hospital.
Source:
http://www.wptv.com/dpp/news/region_c_palm_beach_county/west_palm_beach/explosion-at-palm-beach-county-solid-waste-facility-sends-one-person-to-the-hospital#ixzz1kO4tSJ7Q

23. *January 23, KWQC 6 Davenport* – (Iowa) **Davenport orders $1.1M sewer study.** The city of Davenport, Iowa, recently began conducting sewer studies to find old cracked pipes in the system and where stormwater lines are still connected with sanitary sewer lines, KWQC 6 Davenport reported January 23. All of this leaks extra water into the system. "Right now we're under a consent order from the Iowa Department of Natural Resoures (DNR), and because of that we have to stop exceeding capacity at our treatment plant so we have to do these studies," a plant manager said. "We have a lot of leaking underground in pipes that are causing problems." An increase in sewer fees is being proposed to the city council to pay for this and other projects. The improvements made from these studies will alleviate some of the cost for a $49 million water treatment tank, which is also required by the DNR. The results of the sewer study are expected back in May.
Source: http://www.kwqc.com/Global/story.asp?S=16583351

24. *January 22, Boston Globe* – (Massachusetts) **Road salt worked into Dedham, Westwood water, study finds.** The Dedham-Westwood Water District in Massachusetts is inching closer to its goal of having a section of Route 128 declared a low-salt zone following a study that pegs the state's winter de-icing program as largely responsible for climbing levels of sodium in the drinking water of 38,000 residents in the two towns, the Boston Globe reported January 22. Water district commissioners sought the designation from the state department of transportation for almost a decade since increased salt levels were first discovered in the White Lodge wellfield, one of five operated by the district that lies north of Route 128 near University Avenue. Local officials, including the Westwood town administrator, are concerned about the water's salt content. State guidelines call for drinking water to have a sodium level at or below 20 milligrams per liter (mpl). The Dedham-Westwood Water District said its general distribution system's sodium level is about 60 mpl, while the White Lodge Wellfield has a level of about 100 mpl. Officials said the salt level in the drinking water supply does not pose imminent danger "but is just high enough to be a concern.'' Other than desalinization, the only way to get the salt out of the water is to allow it to dissipate. Communities are responsible for balancing the risks of having salt in the water from ice and snow treatment versus the potential for accidents because of not having the highway sufficiently treated.
Source: http://articles.boston.com/2012-01-22/south/30646148_1_drinking-water-low-salt-road-salt

For another story, see item **37**

[Return to top]

Public Health and Healthcare Sector

25. *January 24, Associated Press* – (Massachusetts) **Dentist accused of paper clip use in root canals.** A former dentist in Fall River, Massachusetts, pleaded guilty to Medicaid fraud for using paper clips instead of stainless steel posts in root canals. Additional charges include defrauding Medicaid of $130,000, assault and battery, illegally prescribing prescription drugs, and witness intimidation. Some of his patients reported

infections after he performed root canals on them, said a spokesman for the state attorney general's office. Prosecutors said the 53-year-old was suspended by Medicaid in 2002, but continued to file claims from August 2003 to June 2005 by using the names of other dentists in his practice. His license to practice dentistry was suspended in Massachusetts in July 2006, and he currently is not licensed to practice dentistry in any state. Authorities said instead of stainless steel posts for root canals, he used sections of paper clips in an effort to save money.
Source: http://www.foxnews.com/us/2012/01/24/dentist-accused-paper-clip-use-in-root-canals/?test=latestnews

26. *January 23, Bloomberg* – (National) **Chemicals used during medical imaging tests may damage thyroid.** Chemicals used to enhance pictures obtained from medical imaging tests may lead to overactive or underactive thyroid glands, a study released January 23 by in the Archives of Internal Medicine showed. Patients injected with contrast material were about twice as likely as those who did not get the chemical to develop hyperthyroidism, when the gland produces too much thyroid hormone and can cause rapid or irregular heart rates. Results also showed an increased risk for hypothyroidism. The use of the chemicals, called iodinated contrast media, has risen in the past two decades as more people get computed tomography scans and heart catheterizations, which are used to diagnose and treat some heart conditions, the researchers said. They looked at patients from January 1990 to June 2010 who did not have any thyroid disease. They also checked to see if they were exposed to iodinated contrast media. They found 178 people developed hyperthyroidism, and, of those, 11 percent received contrast agents. The study also showed 213 developed hypothyroidism and of those, 12 percent received contrast agents. Those who used contrast were 1.5 times more likely than those who did not to develop hypothyroidism, a finding the researchers could not rule out was due to chance.
Source: http://news.businessweek.com/article.asp?documentKey=1376-LY9KLW6JTSEC01-0IFO4CO79V1L7EUJAU5BJT6SMD

27. *January 20, Dexter Daily Statesman* – (Missouri) **Woman charged with lighting bed on fire.** A woman was arrested in Dunklin County, Missouri, January 18 for a November 2011 incident at a Dexter nursing home where a bed of a 73-year-old resident was set on fire with the resident asleep in the bed. According to the Dexter Police Department, the woman admitted to lighting the southeast end of the victim's bed on fire with a lighter and then left the room and went to her cousin's room just down the hall. The woman claims the fire was not premeditated.
Source: http://www.dailystatesman.com/story/1806886.html

For another story, see item **40**

[Return to top]

Government Facilities Sector

28. *January 24, Associated Press* – (California) **Orange County deputies say man crashes into 2 buildings, leaves packages of mineral oil behind.** A man was arrested

January 24 after allegedly crashing his SUV into a social services building and a nearby auto parts store, and leaving behind packages containing mineral oil in Orange, California. The man was booked for investigation of hit-and-run, vandalism, burglary, and facsimile of a weapon of mass destruction, an Orange County Sheriff's Department spokesman said. The man may have targeted social services because of a recent domestic violence arrest, but the connection to the store in Orange was unknown, he told the Orange County Register. The bomb squad was called to both crashes and the areas were cordoned off until the substance could be identified. The man was tracked to his home in Orange after a witness got his license number during the auto parts store crash.
Source: http://www.therepublic.com/view/story/bf2e5ac80a3e4e64b957120ba109fa4b/CA--Building-Crash-Chemicals/

29. *January 24, Global Security Newswire* – (International) **Powder mailings sent to Israeli embassies.** Israeli embassies and consulates at six U.S. and European locations received mailings marked "anthrax" that carried a nontoxic white powder, Agence France-Presse (AFP) reported January 24. The envelopes arrived at Israeli embassies in London, England, The Hague, Netherlands, and Brussels, Belgium, AFP quoted Israeli news reports as saying. Consulates in New York, Houston, and Boston received similar mailings.
Source: http://www.nti.org/gsn/article/suspicious-powder-sent-israeli-foreign-delegations/

30. *January 24, Knoxvlle News Sentinel* – (Tennessee) **Guard allegedly found asleep at Oak Ridge nuke facility.** WSI-Oak Ridge, a security contractor, confirmed January 23 it is investigating allegations a security officer slept on the job and also used an unauthorized cell phone inside a high-security facility at Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee. Photographs of the individual in question were distributed anonymously to multiple groups, including WSI, the Knoxville News Sentinel, and the U.S. Department of Energy (DOE). The photographs were reportedly taken inside Building 3019, the highest-security facility at ORNL. The building houses a large stockpile of fissionable uranium-233. The ORNL director said responsibility for Building 3019 — located in the lab's central campus — has been shifted to the DOE's environmental management organization.
Source: http://www.knoxnews.com/news/2012/jan/24/guard-allegedly-found-asleep-at-oak-ridge-nuke/

31. *January 24, San Francisco Chronicle* – (International) **Solar flare may hit satellite communications, GPS.** A burst of radiation on the sun's surface may trigger a geomagnetic storm on Earth January 24 that could disrupt satellite communications and the Global Positioning System by mid-morning, scientists at the Space Weather Prediction Center said January 23. The eruption — called a solar flare — has also sent billions of tons of matter streaming toward Earth from the sun's surface at millions of miles per hour in what scientists call a coronal mass ejection, according to a physicist at the center in Boulder, Colorado. The radiation storm could create unusually intense flares of the aurora borealis — the northern lights — and has caused some international

airlines to divert planes from polar routes to courses where radio communication is less likely to be affected, the physicist said. A new National Aeronautics and Space Administration satellite called the Solar Dynamics Observatory is vastly improving the ability of scientists to predict the violent magnetic storms that threaten Earth and to understand the mysterious nature of solar physics, the physicist said.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2012/01/24/MNJJ1MTCTM.DTL

32. *January 23, Reuters* – (International) **Senator's Twitter account hacked over piracy bills.** The Twitter account of a U.S. Senator from Iowa was hacked January 23 with bogus tweets attacking his stance on Internet anti-piracy legislation, his office said. He had at least eight false tweets posted as he was on a flight heading from Iowa to Washington D.C., a spokeswoman said. His staff noticed his Twitter account had been broken into a few minutes after the first false tweet was posted and called Twitter to have the password changed.
Source: http://www.reuters.com/article/2012/01/23/us-hacking-senator-grassley-idUSTRE80M28420120123

For another story, see item **47**

[Return to top]

Emergency Services Sector

33. *January 23, Salem Statesman Journal* – (Oregon) **Razor blades found in Marion County jail.** Officials found two contraband straight-edge razor blades at the Marion County, Oregon jail, prompting a search of the facility January 23. How the blades got into the jail is unknown, a sheriff's spokesman said. Inmates can check out safety razors for shaving, but these types of blades — described as straight-edge blades similar to those in box knives — are used in the jail only under heavy supervision to cut linoleum or stair tread, he said. The jail supervisor authorized a cell-by-cell search January 23 after the blades were discovered. The contraband blades apparently belonged to two inmates in different jail pods, the sheriff's spokesman said. About 400 inmates were removed from their cells while law enforcement officers and police dogs searched the facility. Search teams from the Oregon Department of Corrections and Linn County Sheriff's Office helped. The inmates, who were held in a recreation yard for about 7 hours, also were searched individually.
Source: http://www.statesmanjournal.com/article/20120124/NEWS/201240322/Razor-blades-found-Marion-County-jail?odyssey=mod|newswell|text|News|s

34. *January 23, Dothan Eagle* – (Alabama) **Florida man charged with trying to kill trooper.** A Florida man faces an attempted murder charge after authorities said he allegedly tried to kill an Alabama state trooper at a driver's license checkpoint in Geneva County, the Dothan Eagle reported January 23. Court records indicate troopers with the Alabama State Highway Patrol arrested the man the week of January 16 and charged him with felony attempted murder, felony unlawful possession of a controlled substance, and attempting to elude law enforcement. Records indicated he was taken to

the Geneva County Jail and held on $300,000 bail. The Geneva County district attorney said the charges against the man include how he allegedly accelerated his vehicle at the traffic checkpoint while holding on to the trooper's arm, causing the trooper to get dragged down the roadway. The district attorney said the charge also alleged the man turned the wheel of his vehicle in an attempt to have the trooper end up under the vehicle. He said the offense happened as troopers attempted to question the man.
Source: http://www2.dothaneagle.com/news/2012/jan/23/1/man-charged-trying-kill-state-trooper-ar-3099929/

35. *January 23, Levittown Patch* – (Pennsylvania) **Lower Bucks County experiences 9-1-1 problems.** According to emergency management offices in Lower Bucks County, Pennsylvania, the 9-1-1 emergency call center was experiencing problems accepting incoming calls from household landlines. Emergency management offices in Falls Township, Middletown Township, and Tullytown Borough, were among those first reporting problems shortly before the afternoon of January 23. Falls Township officials advised residents who needed to call 9-1-1 for an emergency to use their cell phones to call 9-1-1 or call 215-547-5222. Those in Tullytown were asked to call 215-945-3100 or use their cell phones to call 9-1-1. The issue was only affecting household landlines and not cell phones, according to alerts by area officials. There was no immediate word on the cause of disruption with Verizon's service.
Source: http://levittown.patch.com/articles/lower-bucks-county-experiences-9-1-1-problems

36. *January 23, New York Times* – (National) **Police use of GPS is ruled unconstitutional by court.** On January 23, the Supreme Court unanimously ruled police violated the Constitution when they placed a Global Positioning System tracking device on a suspect's car and monitored its movements for 28 days. A set of overlapping opinions in the case collectively suggested a majority of the justices are prepared to apply broad privacy principles to bring the Fourth Amendment's ban on unreasonable searches into the digital age, when law enforcement officials can gather extensive information without ever entering an individual's home or vehicle. An overlapping array of justices were divided on the rationale for the decision, with the majority saying the problem was the placement of the device on private property. Five justices also discussed their discomfort with the government's use of or access to various modern technologies, including video surveillance in public places, automatic toll collection systems on highways, devices that allow motorists to signal for roadside assistance, location data from cell phone towers, and records kept by online merchants.
Source: http://www.nytimes.com/2012/01/24/us/police-use-of-gps-is-ruled-unconstitutional.html?_r=1&ref=us

For more stories, see items **40** and **47**

[Return to top]

Information Technology Sector

37. *January 24, Wired* – (International) **10K reasons to worry about critical infrastructure.** A security researcher was able to locate and map more than 10,000 industrial control systems hooked up to the public Internet, including water and sewage plants, and found many could be open to easy hack attacks, due to lax security practices. Infrastructure software vendors and critical infrastructure owners have long maintained industrial control systems — even if rife with security vulnerabilities — are not at risk of penetration by outsiders because they are not online. However, a computer science doctoral student from Cambridge University developed a tool that matches information about industrial control systems connected to the Internet with information about known vulnerabilities to show how easy it could be for an attacker to locate and target them. To debunk the myth industrial control systems are never connected to the Internet, the student used the SHODAN search engine, which allows users to find Internet-connected devices using simple search terms. He then matched that data to information from vulnerability databases to find known security holes and exploits that could be used to hijack the systems or crash them. He used Timemap to chart the information on Google maps, along with red markers noting brand devices that are known to have security holes in them. The student found 10,358 devices connected through a search of 2 years worth of data in the SHODAN database. However, he was unable to determine how many of the devices uncovered were actually working systems, nor was he able to determine in all cases whether the systems were critical infrastructure systems installed at power plants and other significant facilities. The student also found only 17 percent of the systems he found online asked him for authorization to connect, suggesting administrators either were not aware their systems were online or had simply failed to install secure gateways to keep out intruders.
    Source: http://www.wired.com/threatlevel/2012/01/10000-control-systems-online/

38. *January 24, Help Net Security* – (International) **Researchers discover network of 7,000 typo squatting domains.** A network of some 7,000 typo squatting domains is being used by scammers to effectively drive traffic towards their sites, some of which get so much traffic that they managed to enter Alexa's top 250 list of sites with the largest Web traffic, according to Websense researchers. The typo squatting domains take advantage of visitors to popular Web sites such as Google, Twitter, Gmail, YouTube, Wikipedia, Victoria's Secret, Craigslist, and many more, and redirect them to spam survey sites. From there, the users are taken to sites with spam advertisements and greyware masquerading as free downloads of legitimate software such as movie downloaders. Websense researchers said currently these sites are not offering malware for download. "However, if these networks are resold to underground groups, then the potential outcome could be even more damaging than the 0-day exploit security attacks," they point out. Users are mostly in danger of handing over their private information and other sensitive data when completing the surveys.
    Source: http://www.net-security.org/secworld.php?id=12275

39. *January 24, H Security* – (International) **Chrome 16 update closes security holes.** Google released version 16.0.912.77 of Chrome which closes several security

holes in the WebKit-based Web browser. The update addresses a total of four vulnerabilities, all of which are rated as “high severity.” These include use-after-free holes in DOM selections and DOM handling, an uninitialized value in the Skia 2D graphics library, and a buffer overflow in tree builder. Four bugs that were detected using AddressSanitizer were also been fixed. The developers note a critical use-after-free issue in Safe Browsing navigation was corrected in version 16.0.912.75 but was “accidentally excluded from the release notes.” Additional details of the vulnerability are being withheld until “a majority of users are up-to-date with the fix.”
Source: http://www.h-online.com/security/news/item/Chrome-16-update-closes-security-holes-1420506.html

40. *January 23, Wired* – (International) **I spy your company’s boardroom.** Researchers from Rapid7 discovered they could remotely infiltrate conference rooms in some of the top venture capital and law firms across the country, as well as pharmaceutical and oil companies and even the boardroom of Goldman Sachs — all by calling in to unsecured videoconferencing systems they found by doing a scan of the Internet. One of the researchers found he was able to listen in on meetings, remotely steer a camera around rooms, as well as zoom in on items to discern paint flecks on a wall or read proprietary information on documents. Despite the fact the most expensive systems offer encryption, password protection, and the ability to lock down the movement of cameras, the researchers found administrators were setting them up outside firewalls and failing to configure security features to keep out intruders. Some systems, for example, were set up to automatically accept inbound calls so users did not need to press an “accept” button when a caller dialed into a videoconference, opening the way for anyone to call in and eavesdrop. Using a program the researchers wrote, they found the conference rooms by scanning the Internet for videoconference systems set up outside firewalls and configured to automatically answer calls. In less than 2 hours, they found systems installed in 5,000 conference rooms, including an attorney-inmate meeting room at a prison, an operating room at a university medical center, and a venture capital company where prospects were pitching their companies while laying out their financial details on a screen in the room. Companies sometimes set up systems outside firewalls so other companies can easily call into the videoconferencing system without having to set up complex, but safer configurations. As a result, the researchers found they could easily hijack systems, and also access systems they otherwise could not find through an Internet scan.
Source: http://www.wired.com/threatlevel/2012/01/videoconferencing-hijacked/

41. *January 23, IDG News Service* – (International) **HP pays $425,000 to settle claims over hazardous laptop batteries.** Hewlett-Packard (HP) will pay $425,000 to settle a claim that it knowingly sold laptops with hazardous batteries that could overheat or catch fire, the U.S. Consumer Product Safety Commission announced January 23. HP learned of about 22 incidents involving the batteries by September 2007, but it failed to report the problem until 10 months later, according to the Commission. The lithium-ion battery packs were shipped in new HP laptops or sold as accessories and spare parts. Because of the defect, they could overheat, posing fire and burn hazards, the Commission said. Soon after it reported the problem, HP and the Commission recalled about 32,000 lithium-ion battery packs. Around the same time, Dell and Toshiba also

recalled lithium-ion battery packs, which were manufactured by Sony. In agreeing to the settlement, HP denied the batteries posed an unreasonable risk or that it violated federal reporting requirements. With respect to the recall, it acted "in accordance with the CPSA and in its customers' best interests," HP said in the agreement.
Source:
http://www.computerworld.com/s/article/9223650/HP_pays_425_000_to_settle_claims_over_hazardous_laptop_batteries?taxonomyId=17

For more stories, see items **1**, **10**, **12**, **16**, **32**, **36**, and **44**

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

42. *January 23, Charlotte Observer* – (North Carolina) **Power glitch hushes radio stations.** A power failure followed by a generator malfunction knocked five Charlotte, North Carolina radio stations off the air for about 4 hours January 21. An operations manager for Clear Channel Radio's five local stations said January 23 that the stations went silent at 11:23 a.m. January 21 when electricity went out in the studios' neighborhood. An emergency generator to power the stations kicked on, but then shut down, he said. Three company engineers came in, backed up a truck used for remote broadcasts to the door of the building and were able to power up key broadcast components from it. By 3 p.m., they had the five stations — WKKT-FM 96.9, WHQC-FM 96.1, WLYT-FM 102.9, WEND-FM 106.5, and WRFX-FM 99.7 — back on the air.
Source: http://www.charlotteobserver.com/2012/01/23/2952639/power-glitch-hushes-radio-stations.html

43. *January 23, KARK 4 Little Rock* – (Arkansas; Texas; Oklahoma) **AT&T wireless service temporarily disrupted in AR, TX & OK.** Some AT&T wireless customers in Arkansas and two neighboring states were affected by a service disruption January 23. It happened for at least a couple of hours during the morning, but all appeared to be back to normal by around 9 a.m. During the disruption, some customers were unable to send or receive text messages. The company released the following statement about the problems: "Earlier today, some customers in North Texas and parts of Oklahoma and Arkansas may have experienced a service disruption with wireless data service. AT&T technicians quickly worked to address the issue, and service is currently running normally."
Source: http://arkansasmatters.com/fulltext?nxd_id=501592

44. *January 22, Santa Fe New Mexican* – (New Mexico) **Damaged cable disrupts Internet service.** Many CenturyLink customers in Santa Fe and other parts of New Mexico were without Internet service for several hours January 23 while Sprint and Virgin Mobile customers across the state were hit by service disruptions through the weekend due to a cut fiber optics cable. Reports of Internet loss began as early as midnight in parts of Santa Fe. CenturyLink reported electrical equipment failure at the Santa Fe office that affected service at 12:45 a.m. January 23, according to CenturyLink's market development manager for Northern New Mexico. By 9 a.m., the system was rebooted, and by 10 a.m. most customers were able to access the Internet again. Sprint and Virgin Mobile customers in Santa Fe, Albuquerque, Farmington, and Los Alamos also were frustrated by interrupted service January 21 through January 22. The culprit was a cut interstate fiber optics cable that affected CenturyLink, according to a regional Sprint communications representative. She said Sprint leases cable space from the cable line in some areas to link service. She confirmed an interstate fiber optics line was cut in Texas, affecting New Mexico. "It impacted the entire state," she said.
Source: http://www.santafenewmexican.com/Local News/Damaged-cable-disrupts-Internet-service

For more stories, see items **31**, **36**, and **38**

[Return to top]

Commercial Facilities Sector

45. *January 24, Associated Press* – (New York) **Repair work may be cause of fatal New York City elevator accident.** New York City's Buildings Department commissioner said maintenance work may have contributed to an elevator accident in which an advertising executive was crushed to death at a 26-story Manhattan office tower, the Associated Press reported January 24. He told the New York Times a maintenance company did repair work on the elevator just before the December 14 accident. He said based on the investigation thus far, the repair work was believed to be a contributing cause, or the cause, of the accident. The Manhattan district attorney also is investigating.
Source: http://www.foxnews.com/us/2012/01/24/repair-work-may-be-cause-fatal-new-york-city-elevator-accident/

46. *January 22, Cincinnati Enquirer* – (Kentucky) **Union carpet store destroyed.** Six fire departments battled a fire for hours January 21 at a carpet store in Union, Kentucky. The Union Fire Department was called to Bill's Carpets Store and called for other units to help after they found dangerous conditions at the standalone building. The rolls of carpet and hardwood flooring stacked inside the building were flammable and were shifting around, the Union fire chief said. Units from six departments responded. Firefighters battled the fire for 8 hours. The cold posed challenges to the more than 50 firefighters who responded. The Transit Authority of Northern Kentucky provided buses for firefighters to stay warm.

Source: http://news.cincinnati.com/article/20120122/NEWS0103/301210035/Fire-destroys-carpet-store?odyssey=nav|head

47. *January 21, Oakland Tribune* – (California) **Officers injured, four arrested in late-night Occupy SF protest.** Four people were arrested January 20 when police and Occupy protesters in San Francisco clashed at a long-closed hotel, leaving some officers injured, authorities said. The violence flared when police confronted hundreds of activists at the Cathedral Hill Hotel. Some protesters occupying the hotel threw objects at police clad in riot gear during the clash, injuring three officers, authorities said. Protesters pulled the fire alarm inside the building, causing police to escort the fire department into the building. Three protesters inside the hotel were arrested for trespassing. The incident occurred at the end of an otherwise peaceful daylong series of protests — called Occupy Wall Street West — in downtown San Francisco. An additional 19 people were arrested early in the day, mostly for blocking an entrance at the Wells Fargo headquarters. One man was arrested for apparently being in possession of a police baton after a brief clash with police. About 200 people stormed the lobby of city hall to stop a foreclosure auction, and more than 1,500 activists flooded 2 streets as darkness fell, snarling the evening commute.
Source: http://www.mercurynews.com/news/ci_19790364?source=rss

For more stories, see items **28**, **38**, and **40**

[Return to top]

National Monuments and Icons Sector

48. *January 23, KVAL 13 Eugene* – (Oregon) **Storm damage closes forest roads.** Weather closed roads across the Willamette National Forest (WNF), Oregon, and efforts to re-open the routes will take days — if not months. Forest Service officials also cautioned travelers to use caution as weather continues to pose the threat of flooding, downed trees, debris flows, and landslides, KVAL 13 Eugene reported January 23. The Aufderheide Drive, Forest Service Road 19, was closed. Crews were working to open one lane. It was expected to be opened by January 24. The slide was above Kiahanie Campground and near the snow line, so it was not blocking access to developed sites or open routes, a WFN spokeswoman said. Blue River Reservoir Road-Forest Service Road 15 was closed. There was major damage to the road — it will not be open anytime soon. The failure on Road 15 was blocking access to the H.J. Andrews Experimental Forest, Mona Campground, and Lookout Campground and Boat Launch. It will likely be several months before the road is re-opened for vehicle access, the Forest Service said. The road leads up to the Blue River Reservoir recreation area, about 3 miles east of Blue River. Forest Service Road 18 (east of Fall Creek) also has a slide. Crews were working to open it up to one lane of traffic.
Source: http://www.kval.com/news/local/Storm-damage-closes-forest-roads-137904183.html

49. *January 23, Merced Sun-Star* – (California) **Rock fall closes road into Yosemite National Park.** A large rockfall that occurred January 22 has closed Highway 120 into

Yosemite National Park in California indefinitely, according to the National Park Service. The road was closed between the Foresta Junction on Highway 120 and the Highway 120/140 Junction. Yosemite was still accessible from Merced and Mariposa via Highway 140, and from Fresno and Oakhurst via Highway 41. The Tioga Road remains closed. Foresta Road, between Foresta and El Portal, was not accessible. Yosemite National Park remains open, but winter driving restrictions are in place on some park roads.
Source: http://www.mercedsunstar.com/2012/01/23/2201944/rock-fall-closes-road-into-yosemite.html

[Return to top]

Dams Sector

Nothing to report

[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