Daily Open Source Infrastructure Report 27 January 2012

Top Stories

- A Kentucky mine was shut down after federal inspectors found two unsecured cases of explosives near a burning pile of coal, loose coal near ignition sources, and inches-thick piles of explosive dust. – *Associated Press* (See item 2)
- A prominent Miami businessman pleaded guilty January 25 to fraud in a $135 million real estate scheme that fleeced hundreds of investors in Florida, New York, and several South American countries. – *Associated Press* (See item 13)

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 25, NewsCore* – (Texas) **Thousands without power after tornadoes, storms slam southeastern Texas.** At least three tornadoes hit southeastern Texas January 25 as severe thunderstorms pummeled the region with strong winds and heavy rains, knocking out power for thousands of residents. The twisters touched down in areas

northwest of Houston, the Houston Chronicle reported, knocking down trees and destroying one local business. Two more tornadoes reportedly touched down in Brenham and in Waller County. High wind gusts before sunrise knocked out power to nearly 21,000 people in the Houston area, with work crews scrambling in the aftermath to restore electricity. Winds and rain also slowed flight arrivals at Houston's George Bush Intercontinental Airport, the Chronicle added.
Source: http://www.myfoxboston.com/dpps/news/texas-tornado-storm-power-dpgonc-20110125-to-_17381001

2. *January 25, Associated Press* – (Kentucky) **MSHA shuts Ky. mine over coal fire, other hazards.** A Kentucky mine was shut down after federal inspectors found two unsecured cases of explosives near a burning pile of coal, as the government issued 174 citations and 19 orders at troubled coal mines during December. The Mine Safety and Health Administration (MSHA) said January 25 it issued 32 citations and 12 orders against Coal Creek Mining LLC's No. 2 Mine in Floyd County, Kentucky. Inspectors found a 5- by 10-foot coal pile on fire about 23 feet from two cases of explosives outside the mine and issued an imminent danger order. The key to the explosives cache was lying on top. Inspectors said they also found a 5-gallon oil bucket full of burning coal and other materials near a portal in the mine, and loose coal up to 30 inches deep under conveyor belts and near ignition sources. The mine was inadequately dusted with pulverized limestone to prevent explosions, and the MSHA said the operator also failed to use approved ventilation plans. Explosive coal dust was 2 to 4 inches deep in places. More unwarrantable failure orders were issued for inadequate hazard examinations, including on-shift conveyor belt examinations and weekly inspections of the return air course and electrical equipment. After the December inspection, the MSHA issued two more orders against Coal Creek for failing to fully correct the problems. The agency also issued 53 citations and five orders in December against Clark Mining Inc.'s No. 3 mine, and 25 citations and two orders against Bell County Coal Corp's Jellico No. 1, both in Kentucky.
Source: http://www.cbsnews.com/8301-505245_162-57366077/msha-shuts-ky-mine-over-coal-fire-other-hazards/

3. *January 25, Associated Press* – (Tennessee) **Coal company sent violation notice over local discharge.** Mining regulators responding to a discharge of partially treated coal cleaning wastewater in the New River in east Tennessee sent a notice of violation letter to Premium Coal Inc, the Associated Press reported January 25. The Tennessee Department of Environment and Conservation issued the letter in response to a January 3 discharge of partially treated coal process wastewater and slurry that includes chemicals used in the washing operation in the Devonia community of Anderson County. The operation remained shut down. No drinking water operations are affected, although there were reports of a black water pollution "plume" more than 28 miles away, said an agency spokeswoman. The discharge originated from a pipe in the Gum Branch Slurry Impoundment and was not reported within 24 hours as required, according to the notice letter signed by an environmental specialist with the mining section of the state agency's water pollution control division. The letter also says the company failed to quickly start collecting discharge water samples. Permit records show there have been violation notices in previous years. The notice orders the

company to continue collecting daily samples and provide detailed water analysis within 30 days. The company in a January 13 report said about 1.4 million gallons of the water "left the impoundment" and an undetermined amount reached the river. Premium Coal's report said its managers "voluntarily idled the preparation plant" and then took corrective action. A member of the board of Statewide Organizing for Community Empowerment said "more than 1 million gallons of toxic waste drained into the New River which flows to the Big South Fork National River and Recreation Area." He said the pollutants "include mercury, selenium, arsenic and all kinds of heavy metals." He also said there were reports of black water just outside the Big South Fork area.
Source: http://www.oakridger.com/newsnow/x364056927/Coal-company-sent-violation-notice-over-local-discharge

For another story, see item **8**

[Return to top]

Chemical Industry Sector

4. *January 25, WFAA 8 Dallas/Fort Worth* – (Texas) **Rainwaters overflow chemical containment ponds in Waxahachie.** Heavy rainfall led state and local officials in Waxahachie, Texas, to respond January 25 to the accidental runoff of chemically polluted waters leftover from a massive chemical spill at the Magnablend plant that occurred last October. One resident saw foam in the air behind his property and smelled a putrid odor. "At this time there are no apparent health threats," said a representative of the Texas Commission on Environmental Quality. "There is a concern that it has discharged into the bayous and ditches in this area, and we are monitoring that." Late January 25, Magnablend officials said the 4 inches of rain had over-run containment ponds established after the October fire destroyed the plant where workers mixed and stored mostly fracking chemicals. Those ponds were presumed to still be polluted with chemical residue. Water samples will be taken by the state and contamination levels will be monitored because the creek leads to the Waxahachie water supply.
Source: http://www.wfaa.com/news/local/Rainwaters-over-top-chemical-containment-ponds-in-Waxahachie-138086863.html

5. *January 25, Philly.com* – (Pennsylvania) **Montco Superfund site owners pay $2.1M.** The current and former owners of a Superfund site in Montgomery County, Pennsylvania, where tires and polyvinyl chloride plastic resins were manufactured, agreed to pay $2.1 million in past cleanup costs, the U.S. Environmental Protection Agency (EPA) announced January 25. The companies — Occidental Chemical Corp. (known as OxyChem), Bridgestone Americas Tire Operations, and Glenn Springs Holdings Inc. — also accepted responsibility for future cleanup costs at the site, which is in Lower Pottsgrove Township. OxyChem currently owns the site, and Glenn Springs manages it. The agreement was spelled out in a consent decree filed in federal court by the Justice Department. For over four decades — 1942 to 1985 — four owners of the property disposed of cutting oils, metal filings, tires, PVC sludge resins, and other wastes. In 1989, the EPA placed the site on its Superfund list because of unsafe

levels of trichloroethylene, vinyl chloride, and other hazardous substances in the soil and groundwater. OxyChem completed remedial action, which included construction of a groundwater treatment plant, and excavating contaminated lagoon sludges in 2008.
Source: http://articles.philly.com/2012-01-25/news/30663453_1_superfund-list-pvc-cleanup-costs

6. *January 25, Environmental Health News* – (West Virginia; Ohio) **Children near West Virginia DuPont plant exposed to higher C8 concentrations than mothers.** Children living near DuPont's plant in Wood County, West Virginia, are exposed to much higher concentrations of an industrial chemical than their mothers, according to a study published online January 23 in the journal Environmental Health Perspectives. Children under 5, exposed from drinking water as well as breast milk, had 44 percent more of the chemical in their blood than their mothers. The study was undertaken by a court-approved panel of three scientists who have spent 7 years trying to determine whether the chemical perfluorooctanoate, or PFOA, also known as C8, is making people sick in the Mid-Ohio Valley. C8 is used in the manufacture of Teflon nonstick cookware, waterproof clothing, food packaging, and other products. Nearly everyone worldwide has traces of it in their bodies. However, people near the DuPont plant have extraordinary levels of PFOA –- about seven times more than the U.S. average –- because the compound, used at the plant since 1951, has contaminated drinking water. For a related chemical called PFOS, blood concentrations were 42 percent higher in children than mothers, and it persisted until the children were 19 years old. Scientists said fetuses, infants, and young children are the most vulnerable to toxic effects of industrial chemicals such as PFOA and PFOS because they might interfere with development of brains, reproductive tracts, and hormones. The panel of scientists was created as part of a settlement after residents from West Virginia and Ohio filed a class action lawsuit against DuPont in 2001 alleging health damage from contaminated water. The panel is scheduled to reach a conclusion in July about the probability of health effects from PFOA exposure. Under the settlement, if the scientists find a "probable link" exists between the chemical and any diseases, DuPont will fund a medical monitoring program for residents.
Source: http://www.environmentalhealthnews.org/ehs/news/2012/c8-found-in-high-concentrations-near-west-virginia-dupont-plant

[Return to top]

Nuclear Reactors, Materials and Waste Sector

7. *January 26, Nashville Tennessean* – (Tennessee) **Regulators say flood barriers may not protect TVA's nuclear plants.** Sand baskets that the Tennessee Valley Authority installed at dams in Tennessee to protect its nuclear plants from a worst-case flood could fail, according to a Nuclear Regulatory Commission (NRC) letter dated January 25. The NRC said the baskets are not capable of standing up to the impact of debris barreling down the Tennessee River in a massive flood. "There is potential for this debris to damage the baskets or push the individual baskets apart, causing a breach," the letter said. "There would be no time to repair the baskets because the flood would already be in progress." The sand-filled, wire mesh baskets were placed around

Cherokee, Fort Loudon, Tellico, and Watts Bar dams and earthen embankments. The electric power producer had told the NRC in 2010 that a project to resolve flooding concerns would extend into 2016 with dam modifications handled by the U.S. Army Corps of Engineers. Lack of federal funds is expected to cause more delay. The NRC said the baskets are acceptable as a temporary fix.
Source:
http://www.tennessean.com/article/20120126/NEWS11/301260077/Regulators-say-flood-barriers-may-not-protect-TVA-s-nuclear-plants?odyssey=nav|head

[Return to top]

Critical Manufacturing Sector

8. *January 25, WJXT 4 Jacksonville* – (Florida) **Rechargable battery plant evacuated.** A new rechargeable battery manufacturing plant in Jacksonville, Florida, was evacuated January 25, and two people were hospitalized after they were apparently overcome by fumes. More than 100 people were ordered out of one building that was evacuated. In addition to two people being transported to area hospitals, six people were evaluated for effects from exposure. A haz-mat team went through the building with air monitors, and an all-clear was given just before 4:30 p.m.
Source: http://www.news4jax.com/news/Rechargable-battery-plant-evacuated/-/475880/8501726/-/ig65hyz/-/index.html

9. *January 25, Associated Press* – (Georgia) **Pa. company fined $93K for Ga. plant.** A Rydal, Georgia manufacturing plant that manufactures heavy duty truck bodies for Home Depot, Lowe's, UPS, FedEx, and Ryder was fined $93,000 for what federal officials said were safety and health violations, the Associated Press reported January 25. The Occupational Safety and Health Administration said Morgantown, Pennsylvania-based Morgan Corp. failed to provide welding screens for workers and did not give employees training on how to use hazardous chemicals, among other infractions. Other violations included workers who were allowed to bypass safety features on equipment. In all, federal officials said the plant had 24 violations following a July inspection visit.
Source: http://www.canadianbusiness.com/article/67624--pa-company-fined-93k-for-ga-plant

[Return to top]

Defense Industrial Base Sector

See item **8**

[Return to top]

Banking and Finance Sector

10. *January 25, KPHO 5 Phoenix* – (Arizona) **Guilty plea from 'Black Binder Bandit'.** A man who confessed to a dozen bank robberies in the East Valley area of Arizona pleaded guilty in federal court January 24. The defendant faces a maximum of life in prison and a $250,000 fine. Investigators dubbed the man the "Black Binder Bandit" because he frequently carried a black binder that contained a note and sometimes a gun. He would also place the money in the binder before leaving the bank. He admitted to robbing 12 banks starting September 2, 2010, until he was arrested July 20, 2011. He said he made off with more than $49,000 in those robberies.
Source: http://www.kpho.com/story/16600659/guilty-plea-from-black-binder-bandit

11. *January 25, St. Louis Post-Dispatch* – (Missouri) **St. Louis County police arrest suspect in 'Logo Bandit' bank robbery.** A man from Mexico, Missouri, was charged January 25 in a bank robbery earlier this month blamed on a man authorities dubbed the "Logo Bandit," police said. He was charged with robbery for the January 17 holdup of Jefferson Bank and Trust. The suspect in the Jefferson Bank robbery implied he was armed but never displayed a weapon. According to court documents, he said he went into the bank and gave a teller a note with the word "robbery" on it. Police said he kept a hand inside his jacket and implied he had a gun. He ordered the teller to give him $100 and $50 bills from the drawer and "not to attempt any funny stuff and nothing will happen." After the teller put $3,670 on the counter, he took the money and left, court documents say. Police arrested the suspect in Richmond Heights with help from the FBI and the Richmond Heights Police Department. He could be charged in other municipalities where he is suspected in bank robberies, police said. Police and the FBI have suspected the "Logo Bandit" in at least seven other bank robberies over the past 4 months. He was given the nickname because he wore hats and sweatshirts featuring brand-name or athletic logos each time he robbed a bank.
Source: http://www.stltoday.com/news/local/crime-and-courts/st-louis-county-police-arrest-suspect-in-logo-bandit-bank/article_c1f07f36-4790-11e1-b9b2-001a4bcf6878.html

12. *January 25, KOVR 13 Sacramento* – (California; Nevada) **'Fedora Bandit' charged with 7 Northern California bank robberies.** The suspect dubbed the 'Fedora Bandit" was charged with seven counts of armed bank robbery in California January 24, a U.S. attorney announced. According to court documents, the suspect also committed the April 12, 2010 armed robbery of the Bank of the West's Carson City, Nevada branch. He is currently in federal custody in Lompoc on a drug trafficking conviction after being stopped in a motor home in Kansas in December 2010 with more than 40 pounds of cocaine, and more than 160 pounds of marijuana. According to the FBI criminal complaint, he confessed to the bank robberies while being interviewed at the federal penitentiary January 19. He faces up to 25 years in federal prison for each armed bank robbery. The suspect, who earned the nickname because of the fedora-style hat he wore during alleged heists, made off with a reported $56,000 in cash from the California bank robberies.
Source: http://sacramento.cbslocal.com/2012/01/25/fedora-bandit-charged-with-7-northern-california-bank-robberies/

13. *January 25, Associated Press* – (Florida; New York; International) **Prominent Fla. businessman guilty in $135M fraud; investors include Roman Catholic prep school.** A prominent Miami businessman pleaded guilty January 25 to fraud in a $135 million real estate scheme that fleeced hundreds of investors, including the Roman Catholic prep school he once attended. He faces up to 5 years behind bars after pleading guilty to a single count of wire and mail fraud conspiracy. He also lured investors from Miami's close-knit Cuban-American community, many of them elderly and some Roman Catholic priests. Federal prosecutors said the man operated his company, Royal West Properties Inc., like a Ponzi scheme in which he paid older investors with money raised from newer ones. The company sold real estate investments in southwest Florida since 1993, but fell on hard times beginning in 2002 and was eventually forced into bankruptcy in 2009, according to court documents. Before it crashed, Royal West promised rates of return as high as 16 percent for investors who bought properties that were marketed nationally on Spanish-language networks and through offices in Florida, New York, Colombia, Ecuador, Peru and Venezuela. The chief of the Securities and Exchange Commission field office in Miami, called it a typical "affinity" scam where the perpetrator uses a position of trust to prey on members of a specific group. In all, prosecutors said more than 150 investors lost about $47 million between 2003 and 2008. Of the total, investigators said the man and his wife skimmed about $20 million for other business ventures, to pay themselves more than $5 million in salaries, and to pay children and grandchildren $1 million in "consulting fees" even though they did no work for Royal West. He could be ordered to pay millions of dollars in restitution.
Source: http://www.washingtonpost.com/business/prominent-fla-businessman-guilty-in-135m-fraud-investors-include-roman-catholic-prep-school/2012/01/25/gIQApE8aQQ_story.html

14. *January 25, U.S. Department of Justice* – (Florida) **Former executive of Miami-based ocean bank pleads guilty to participating in bribery scheme and to fliing false tax returns.** A former executive of Miami-based Ocean Bank pleaded guilty January 25 in a U.S. district court in Miami to participating in a scheme to accept bribes and to failing to report the income on federal income tax returns, the Department of Justice announced. The charges against the former vice president stemmed from his accepting nearly $500,000 in cash and other items from unnamed co-conspirators in connection with his supervision of certain unnamed customer business with the bank. According to court documents, the vice president generally oversaw Ocean Bank's lending relationships with corporate customers. The department said that beginning in or about February 2001 and continuing thereafter through on or about April 25, 2007, he accepted bribes, including payments for expensive watches, Super Bowl tickets, and other items for his personal use, as well as substantial amounts of cash. He accepted the payments intending to be rewarded and influenced in connection with his role in approving Ocean Bank's issuance of letters of credit, loans, and overdraft privileges to co-conspirators. The court documents also show he failed to report income from the bribes for the tax years 2005, 2006 and 2007, resulting in lost tax revenue of about $91,000 to the federal government. He was charged with one count of conspiracy to solicit or demand money and other things of value to influence an employee of a financial institution and three counts of tax offenses. The conspiracy count carries a

maximum sentence of 5 years in prison and a $250,000 criminal fine. The tax charges each carry a maximum sentence of 3 years in prison and $250,000 fine.
Source: http://www.justice.gov/opa/pr/2012/January/12-at-102.html

For another story, see item **46**

[Return to top]

Transportation Sector

15. *January 26, Associated Press* – (Texas) **11 hurt, none seriously, in Dallas bus crash.** Eleven people have been hospitalized after a tractor-trailer rig crashed into the rear of a Dallas public transit bus. A Dallas Area Rapid Transit (DART) spokesman said the bus was rear-ended around 4 p.m. January 25 on Loop 12, about 1 mile west of U.S. 175 in southeast Dallas. The 10 passengers on the bus and the bus driver suffered primarily back and neck injuries. All were hospitalized, although the spokesman said none of the injuries are serious.
Source: http://abclocal.go.com/ktrk/story?section=news/state&id=8519531

16. *January 26, WFAA 8 Dallas/Fort Worth* – (Texas) **Drivers become stranded in high waters across North Texas.** Several high-water rescues were reported throughout the morning January 25 as flooding stalled vehicles across North Texas. The frontage roads off Interstate 635 at Park Central were closed off in both directions due to flooding. Water was so high, the ground could not be seen at Anderson Bonner Park and the White Rock Creek and Trail were completely under water in Dallas. In Haltom City, a swift water rescue was reported in the 5900 block of Midway Road at the underpass of Highway 121 heading out of Fort Worth. Three vehicles became stuck, with two of the drivers able to wade back to safety. The third driver was rescued on a swift water boat. Haltom City officials said the Midway Road rescue was their second of the day near Big Fossil Creek. At least five cars stalled out at Trinity Boulevard between Precinct Line Road and Norwood Drive in Fort Worth. Water was reported to be knee-deep and vehicles remained stuck for hours before crews began to move them off the road. The Venus Independent School District in Johnson County was closed for the day due to high waters making it difficult for drivers to get to the school.
Source: http://www.wfaa.com/home/Steady-Rain-Causes--Rising-Water-in-North-Texas-138032493.html

17. *January 25, Seattle Times* – (Washington) **Windy night closed 520 bridge for 40 minutes of maintenance.** The 520 bridge in Seattle was closed briefly twice early January 25 when strong winds knocked some bridge finger plates loose in the westbound lanes of the span. Emergency work closed the bridge for about 30 minutes starting at midnight for repairs to one portion of the span. The bridge was closed 10-15 minutes starting at 1 a.m. to repair another portion, according to a Washington State Department of Transportation spokesman. Alarms on the bridge were triggered by the winds, alerting crews that were on standby that something was wrong, he said. Bolts holding the finger plates (the metal expansion joints between sections of the bridge) had come loose and needed to be replaced. The span's drawbridges had to be raised so

maintenance crews could work on them, the spokesman said. Wind gusts reached about 47 miles per hour. Generally, the state closes the bridge when sustained winds reach 50 miles an hour for 15 minutes.
Source: http://today.seattletimes.com/2012/01/windy-night-closed-520-bridge-for-20-minutes-of-maintenance/

18. *January 25, Detroit Free Press* – (Michigan) **MDOT's aeronautics office overlooked expired licenses at 5 flight schools, report says.** An audit released January 24 said the Michigan Department of Transportation's (MDOT) Office of Aeronautics let 5 of 63 Michigan flight schools operate with expired state licenses. The report said four of the schools had licenses that expired December 31, 2010, and one had a license that expired December 31, 2009. Licenses must be renewed annually. "The Office of Aeronautics failed to detect that these five schools had not submitted renewal applications," and therefore the schools continued to operate out of compliance with state law, the audit said. The report did not identify the flight schools, but a MDOT spokesman identified them as Benz Aviation in Ionia and Grand Haven, Blue Sun Air in Zeeland, Flying Tiger in Marquette, Hillsdale Aero in Hillsdale, and Crosswinds Aviation in Howell. State licenses for all five facilities remained lapsed as of January 24, he said. The audit also said that for 79 percent of the schools, state officials did not complete inspections within 3 years, as required. For eight of the schools, inspections were more than 5 years behind schedule, the report said. Inspections were 3 to 5 years late for 26 schools, 1 to 3 years late for 12 schools, and a year or less late for 4 schools. The department did not dispute the findings but promised to fix the problems.
Source: http://www.wzzm13.com/news/article/196250/14/Report-MDOTs-office-overlooked-expired-licenses-at-flight-schools

For more stories, see items **19**, **34**, and **48**

[Return to top]

Postal and Shipping Sector

19. *January 25, The White House Blog* – (National) **National strategy for global supply chain security announced.** Pandemics, natural disasters, or attacks involving weapons of mass destruction could undermine the continuity of the global supply chain system as a whole. Because of the interconnectedness of the system, even smaller, localized events could escalate rapidly and cause significant disruptions. The White House announced January 25 the National Strategy for Global Supply Chain Security, an important step to strengthen and protect the global supply chain system. The strategy, focused on the worldwide network of transportation, postal, and shipping assets and supporting infrastructures, articulates the nation's vision and approach, and encourages collaborative implementation with key state, local, tribal, territorial, private sector, and international stakeholders.
Source: http://www.whitehouse.gov/blog/2012/01/25/national-strategy-global-supply-chain-security-announced

[Return to top]

Agriculture and Food Sector

20. *January 26, KHOU 11 Houston* – (Texas) **Police arrest alleged serial 'sandwich shop robber' after attempted Subway holdup in the Heights.** An alleged serial robber who has been targeting sandwich shops in the Heights area of Houston was arrested January 25, police said. Investigators said the suspect robbed at least six businesses since November. The businesses included two Subways and a Quiznos. Officers were watching two shops the crook hit multiple times. Police nabbed him when he allegedly tried to hold up a Subway at gunpoint January 25. They said he hit that same shop at least three times before.
Source: http://www.khou.com/news/crime/Police-arrest-alleged-serial-sandwich-shop-robber-138100143.html

[Return to top]

Water Sector

21. *January 26, Half Moon Bay Review* – (California) **Dual sewage leaks contaminate Surfer's Beach.** The San Mateo County Environmental Health Department in California closed Surfer's Beach January 25 following a main break that spewed roughly 1,000 gallons of untreated sewage, possibly contaminating local waters. It was not clear what caused the incident or if Surfer's Beach water quality was affected, explained the director of environmental health. Sewer Authority Midcoastside (SAM) crews fixed the sewage release but the spill triggered a beach closure until water samples indicate sewage did not seep to the ocean. The spill follows a similar incident January 21 in which heavy rains blocked up one of SAM's sewage mains. The initial weekend spill resulted in the release of about 2,000 gallons of untreated sewage. Though authorities did not think the spill flowed to the ocean, they closed the beach and immediately began sampling the water. Results that came back January 22 indicated levels slightly above state standards for beaches. Officials were unsure if the incidents were related. Samples should be available January 26.
Source: http://www.hmbreview.com/news/dual-sewage-leaks-contaminate-surfer-s-beach/article_9a17c9bc-47c0-11e1-b1ed-001871e3ce6c.html

22. *January 25, City of San Marcos Water/Wasterwater Utility* – (Texas) **Downpour spills sewage into San Marcos River.** The San Marcos Water/Wastewater Utility in San Marcos, Texas, reported an overflow of an estimated 800,000 gallons of domestic wastewater diluted with rainwater into the San Marcos River following nearly 5 inches of rain within a 4 hour period overnight January 25. The overflow occurred just outside the main lift station. The discharge lasted about 6 hours, according to the assistant director of public services. The area potentially affected by the discharge is the San Marcos River downstream of the Interstate 35 bridge across the river.
Source: http://smmercury.com/53175/downpour-spills-sewage-into-san-marcos-river/

23. *January 24, Columbia State* – (South Carolina) **Untreated wastewater spills into Stoop Creek.** Sewage backed up behind a grease-and-roots blockage spilled for nearly 3 days from a residential sewer system near Stoop Creek in Columbia, South Carolina,

before it was fixed January 23. Palmetto Wastewater Reclamation reported the volume of the spill as much greater than 5,000 gallons. Flow through small sewage lines varies between almost none to 20 gallons per minute, depending on the time of day and Palmetto suspects sewage had been flowing to some degree from a manhole. A resident noticed a bad smell in that area January 20, according to a spokesman. Officials said residents should avoid contacting the water of Stoop Creek downstream of the leak, which is downstream from Harbison State Forest. The creek runs from there through St. Andrews for several miles before eventually dumping into the Saluda River.
Source: http://www.thestate.com/2012/01/24/2126097/untreated-wastewater-spills-into.html

For more stories, see items **3**, **4**, **5**, and **6**

[Return to top]

Public Health and Healthcare Sector

See items **28**, **29**, and **41**

[Return to top]

Government Facilities Sector

24. *January 26, Associated Press* – (Maryland) **Md. man caught in sting pleads guilty in bomb plot.** A Maryland man pleaded guilty January 26 to trying to detonate what he thought was a car bomb outside a military recruiting center in suburban Baltimore. He said he was motivated by what he saw as an American war on Islam. The man entered the guilty plea to the charge of attempting to use a weapon of mass destruction against federal property. The plot to bomb the Armed Forces Recruiting Center in Catonsville in December 2010 was foiled by an FBI sting. The man had also faced a charge of trying to kill U.S. officers and employees, but prosecutors agreed to drop the second charge at sentencing. The deal calls for a 25-year prison term.
Source: http://www.wvnstv.com/story/16606675/md-man-caught-in-sting-pleads-guilty-in-bomb-plot

25. *January 25, Government Computer News* – (International) **FTC site still down after Anonymous hack; anti-piracy fallout spreads.** The Federal Trade Commission's (FTC) cybersecurity advice Web site remained offline January 25, a day after it had been hacked by the group Anonymous in a continuing protest over proposed anti-piracy laws and recent anti-piracy arrests. The OnGuardOnline.gov site, intended to give people cybersecurity advice, was hacked January 24, with the home page replaced by the Anonymous logo, a rap song, and a message threatening more attacks if anti-piracy legislation in Congress, which has stalled after a massive online protest January 18, were to pass. The FTC, which operates the site with several other agencies, took it offline after the hack.
Source: http://gcn.com/articles/2012/01/25/ftc-anonymous-hack-sopa-megaupload-fallout.aspx

26. *January 25, WREG 3 Memphis* – (Tennessee) **North Panola student injured in acid attack.** A student was recovering from surgery January 25, that he needed to have after officials said another student threw acid on him during an incident at North Panola High School in Memphis, Tennessee. The conservator of the North Panola School District said it happened during an in-school suspension period, where the victim and two other students were in the room. A teaching assistant, who was in the room, was supposed to be monitoring the students. That aide has now resigned. Authorities could not find the container for the chemical used, but the conservator said it is possible a student could have located material misplaced by workers during construction. The school is currently undergoing renovations, including in the science lab areas. The student accused of throwing the acid was suspended pending further investigation. He could be subject to further disciplinary action. School authorities have gone through the school to make sure no harmful materials are accessible to students.
Source: http://www.wreg.com/news/wreg-north-panola-student-injured-in-acid-attack-20120125,0,6038477.story

27. *January 25, Reuters* – (Texas) **Secret Service: Man detained at a former President's home had gun.** A man detained outside the home of a former U.S. President had a weapon in his car but was released after questioning January 24, a U.S. Secret Service spokesman said January 25. The spokesman said the man told agents and Dallas police that he was spiritually told to pick up a package at the former President's home. He had a permit to carry a gun, which was found in his vehicle. The spokesman said neither the former President nor his wife were at the house at the time.
Source: http://www.reuters.com/article/2012/01/25/us-bush-home-dallas-idUSTRE80O1MA20120125

28. *January 25, WJXT 4 Jacksonville* – (Florida) **39 Duval County Health Department staffers feel ill.** More testing was being done for airborne contaminants at the Duval County Health Department in Jacksonville, Florida, after 39 staffers complained of ill effects from exposure to some airborne agent in the building, WJXT 4 Jacksonville reported January 25. Six staffers went to the doctor, and two were hospitalized. The effects included headaches, dizziness, eye irritation, and fatigue. The problem is believed to have stemmed from a leak on the second floor of the building January 13. City officials said a glass drain pipe often used to dispose chemicals in the health department's laboratory broke, causing the leak. It was fixed the same day, and that was when the complaints started. Staffers said the odor smelled like cleaning products. Officials were doing a comprehensive air monitoring for 8 hours January 25. Results were expected back the week of January 30.
Source: http://www.news4jax.com/news/39-Duval-County-Health-Department-staffers-feel-ill/-/475880/8499690/-/15u682x/-/index.html

29. *January 25, Nextgov.com* – (National) **Symantec software upgrade caused Military Health Record System shutdown.** The Military Health System (MHS) identified Symantec's Veritas Storage Foundation storage software as the cause of a shutdown of the Armed Forces Health Longitudinal Technology Application (AHLTA) clinical data repository (CDR), which stores 9.7 million electronic records for active-duty and retired military personnel and their families, NextGov reported January 25. The

Defense Information Systems Agency (DISA) also acknowledged it played a key role when the AHLTA CDR shut down. MHS said it took the CDR offline for most of the day January 17 to correct a problem with an upgrade to storage service software that was loaded over the 3-day Martin Luther King Jr. weekend. An MHS spokesman said the problem experienced with the upgrade was an issue fixed in the previous version but was not included in the current CDR operating system. She said Symantec is developing a patch, which is expected to be delivered within 2 weeks. During the interim, AHLTA will run on the older version of the software. The DISA operates a backup repository for the MHS in San Antonio, but after the failure of the primary system, the agency did not revert to that backup site at the direction of the MHS. Instead, AHLTA users were switched to local mode with backup cache servers while the problem was addressed.
Source: http://www.nextgov.com/nextgov/ng_20120125_1271.php

30. *January 25, Federal Times* – (National) **More than 4,000 vets potentially affected by VA data breach.** A Veterans Affairs (VA) Department data breach may have put at risk the personal information of more than 4,000 veterans, the VA Chief Information Officer said January 25. That is nearly twice the number of potentially affected vets VA said the week of January 16 were eligible for credit monitoring because of the breach. The information, including Social Security numbers, was posted on Ancestry.com last March and not discovered by VA until December, 8 months later, when the daughter of a living veteran complained personal information about her parent had been posted on the Web site. The information was immediately taken off the Web site in December. The VA had confirmed the personal data of at least 2,257 living veterans was mistakenly released to Ancestry.com as part of a response to a Freedom of Information Act request involving 14.7 million veteran records. VA is now reviewing about 2,000 additional names to determine if the individuals are deceased or living.
Source:
http://www.federaltimes.com/article/20120125/DEPARTMENTS04/201250304/

For another story, see item **16**

[Return to top]

Emergency Services Sector

31. *January 26, Atlanta Journal-Constitution* – (Georgia) **Georgia officials search for fake fire inspector.** The Marietta Fire Department in Marietta, Georgia, is looking for a man pretending to be a city fire inspector who is charging local businesses for fire inspections, the Atlanta Journal-Constitution reported January 26. The Marietta fire marshal said the city requires annual inspections and fire extinguisher checks, but does not charge for them. He said one business paid a man dressed in dark pants and a blue shirt, similar to the firefighter's uniform, $50 for a bogus inspection.
Source: http://www.firehouse.com/news/10618723/georgia-officials-search-for-fake-fire-inspector

32. *January 25, Associated Press* – (Lousiania) **Eunice man back in jail again for allegedly impersonating a police officer.** A 57-year-old man from Eunice, Louisiana, arrested in November for impersonating a police officer is back in jail again and facing the same charge, the Associated Press reported January 25. The Eunice police chief told the Opelousas Daily World that the suspect, who is being held without bail, was booked with theft, false impersonation of a police officer, and three counts of threatening a public official. He said the suspect was arrested over the weekend of January 21 on a charge of shoplifting at a local store. The suspect identified himself as a St. Landry Parish Sheriff's Office deputy several times and threatened to have the arresting officers' jobs. The police chief stated the suspect was employed by the sheriff's office briefly in 2005.
Source:
http://www.therepublic.com/view/story/a44fe657c3914c80b413e1db63aece3c/LA--Police-Impersonator/

33. *January 25, Orlando Sentinel* – (Florida; International) **Ex-UCF student pleads guilty to federal hacking charge.** The Orlando Sentinel reported January 25 that a former student of the University of Central Florida (UCF) in Orlando, Florida, charged with hacking into a Web site used by the FBI recently pleaded guilty in federal court, records show. The former student was arrested at his dorm on the UCF campus in July after investigators said he hacked into the Tampa Bay InfraGard site in June and uploaded three files. Minutes after the unauthorized intrusion, federal prosecutors said, he posted a thread on a hacker forum Web site that provided a link to InfraGard and instructions on how to exploit the site. Soon after his posting, at least 15 hacking attempts were made on the Web site, 7 of them being successful, court records said. The records also said the former student, using the Twitter name "voodooKobra," sent a message to the FBI's press office Twitter account stating InfraGard "has one hell of an exploit." He was arrested on a federal hacking charge July 19. Documents filed by prosecutors said he confessed to hacking into the InfraGard site. Records show he pleaded guilty in federal court in Tampa the week of January 16, and a judge accepted the plea and adjudicated him guilty January 20. The man faces up to 5 years in federal prison, up to 3 years probation, and a fine of up to $250,000.
Source: http://articles.orlandosentinel.com/2012-01-25/news/os-ucf-hacker-pleads-20120125_1_ucf-student-federal-court-plea-and-adjudicated

34. *January 25, Associated Press* – (Virginia) **Va. Beach man pleads guilty to shining green laser at police helicopter during manhunt.** A man from Virginia Beach, Virginia, pleaded guilty in federal court January 25 to interfering with someone operating an aircraft after he acknowledged shining a green laser at a police helicopter as it searched for a fleeing suspect. Federal prosecutors said it was the first felony conviction in a laser-pointing case within the Eastern District of Virginia, although local and federal officials said the use of the inexpensive laser pointers against aircraft is a growing problem. State lawmakers are considering making it a state crime to project a laser at an aircraft, though federal officials said they would keep up the pressure on those who threaten pilots' safety. Prosecutors said the man recklessly endangered pilots flying a Virginia Beach police helicopter by shining his laser at them from his backyard for about 20 minutes, hitting one of the pilots in the left eye at one

point. The pilot was unable to monitor the helicopter's instruments and on three occasions the crew had to stop pursuing the suspect they were originally chasing due to the unsafe conditions the laser created, court records show. Following his guilty plea, the man apologized to police at a news conference and he spoke about the dangers of using lasers. He faces a maximum penalty of 20 years in prison when he is sentenced May 18.
Source: http://www.washingtonpost.com/local/va-beach-man-pleads-guilty-to-shining-green-laser-at-police-helicopter-during-manhunt/2012/01/25/gIQAJzc7QQ_story.html

[Return to top]

Information Technology Sector

35. *January 26, V3.co.uk* – (International) **Symantec advises users to turn off pcAnywhere in hack aftermath.** Symantec has advised customers to take their copies of pcAnywhere offline as the company continues to struggle with the aftermath of a major data breach. The company issued a whitepaper addressing new vulnerabilities in its remote access tool that were exploited by a recently publicized attack which allowed attackers to gain access to the application's source code. The 2006 hack was recently brought to light by an Indian hacking team that is seeking to publicly distribute the code. Symantec has now determined a major update is necessary to protect users from any flaws revealed in the compromised source code. The company is advising users of pcAnywhere 12.5 to disable the remote management tool until an update is released. If users do not take their copies of the tool offline, the company warned attackers could possibly compromise systems and perform "man-in-the-middle" attacks that could result in the theft of user credentials and other network traffic.
Source: http://www.v3.co.uk/v3-uk/news/2141452/symantec-advises-users-pcanywhere-hack-aftermath

36. *January 26, Computerworld* – (International) **Google stirs up privacy hornet's nest.** Google announced the company is rewriting its privacy policy, consolidating user information across its services. The company, however, is not offering users an opt-out option. If a user does not want their information from Gmail, YouTube, and Google searches combined into one personal data store that can paint a detailed picture of them, the only option is to cease using Google's services.
Source:
http://www.computerworld.com/s/article/9223719/Google_stirs_up_privacy_hornet_s_nest?taxonomyId=17

37. *January 25, Threatpost* – (International) **Poison Ivy variant changes benign code to malicious after download.** Researchers found there are now some pieces of malware downloading not explicitly malicious pieces of code, but small bits of code benign on their face that are then transformed into malicious instructions once they are on the target machine. The code was found by Microsoft researcherst when investigating a file calling out to the site of a restaurant. They expected the file to be a standard downloader that would pull down a malicious executable hosted on the compromised server and then run that locally. Instead, the file was downloading a piece of code that

did not do much at first. Further analysis showed the initial VisualBasic application was doing many things. “Once the application was run on a machine with a simulated Internet connection, it got the contents of the HTML page of the restaurant website mentioned previously. The application copied itself to the Windows system folder as ‘misys.exe’, and started keylogging, although the static analysis did not indicate this kind of functionality,” Microsoft researchers wrote in an analysis. “So the VB Application is extending its functionality dynamically by downloading and executing x86 instructions in the context of its own process. The ‘downloader’ becomes malware by executing this downloaded blob of x86 instructions. And the downloaded instructions will be not injected to a different process and not dropped to disc, they will be executed in the process context of the ‘downloader’, thus the ‘downloader’ inherits the malware functionality.” What the victim ends up is a version of the Poison Ivy backdoor.
Source: http://threatpost.com/en_us/blogs/poison-ivy-variant-changes-benign-code-malicious-after-download-012512

38. *January 25, Softpedia* – (International) **Amateur programmer: SMS spoofing for malicious purposes is easy.** SMS spoofing is not new, researchers having proved in 2010 for BBC’s Watchdog it could be done. While most telecommunications companies are aware of the risks, few have actually done something to prevent it. Now, an amateur programmer came forward with a simple app to prove SMS spoofing for malicious purposes is something widely available, and if measures are not taken, a lot of individuals may be exposed to cybercriminal operations. A self-described “completely amateur programmer” with less than 2 years’ experience, managed to develop a simple program that could allow anyone to launch social engineering attacks with the purpose of obtaining valuable information and maybe even money.
Source: http://news.softpedia.com/news/Amateur-Programmer-SMS-Spoofing-for-Malicious-Purposes-Is-Easy-248669.shtml

For more stories, see items **25**, **33**, **39**, and **46**

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

39. *January 26, Dark Reading* – (International) **Hacktivists turn to DNS hijacking.** Hacktivists have added a new tactic to their arsenal: redirecting all traffic from a target company’s Web site, Dark Reading reported January 26. According to a blog written by a security expert from Internet Identity (IID), politically motivated attackers are now using DNS hijacks, which redirect all traffic from a victim’s

legitimate Web site (and often all the e-mail and back-end transactions, too) to a destination of the attacker's choosing. "A determined criminal can set up a fake look-alike destination site to dupe customers into revealing credentials or downloading malware," the expert stated. Many companies pay little, if any, attention to securing their domain registrations, and most do not continuously monitor their DNSes to make sure they're resolving properly around the world, making them vulnerable to attack, the blog said. "The first indication most victims have of a DNS hijack is that their website traffic slows to a trickle," it noted. "Then they have to figure out why, and DNS is rarely the first thing they think of, which lengthens the time to mitigate the attack." On January 22, the domain name UFC.com was hijacked by a hacktivist group, IID reported. On January 23, that same group, called UGNazi, hijacked two domain names, coach.com and coachfactory.com, belonging to luxury goods maker Coach Inc. Both Coach and UFC registered their domains at Network Solutions, IID reports. "The criminals hijacked the domains by accessing the companies' domain management accounts at Network Solutions," the blog stated. "It's currently unclear how they did so. In such cases, the cause is usually weak or compromised user passwords, or a website vulnerability at the registrar."
Source: http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232500513/hacktivists-turn-to-dns-hijacking.html

40. *January 25, KRBD 105.3 FM Ketchikan* – (Alaska) **KPU phone experiences outages.** About 50 percent of Ketchikan Public Utilities (KPU) telecommunications customers in Alaska experienced a telephone outage January 25. At about 8:45 a.m., some KPU residential and business customers began experiencing fast busy signals, could not get a dial tone, or reached "call cannot be completed" recordings when attempting to place calls. There were periods of time when KPU customers were able to make and receive calls, only to have the call terminated. The outage also affected some cellular customers and those serviced by other phone carriers trying to call KPU customers. KPU's Internet and TV services were not affected. The source of the outage was located in KPU's central computerized switching network. KPU technicians worked with the manufacturer of the switching network to restore service. Service was restored to all customers at about 2 p.m. January 25.
Source: http://www.krbd.org/2012/01/25/kpu-phone-experiences-outages/

For more stories, see items **8**, **36**, and **38**

[Return to top]

Commercial Facilities Sector

41. *January 26, Salt Lake Tribune* – (Utah) **Man surrenders after standoff inside SLC pharmacy.** Salt Lake City police closed a Rite Aid store January 25 for several hours after a man allegedly entered carrying a Molotov cocktail and barricaded himself in the pharmacy area. The man was taken into custody after he was talked into surrendering by police negotiators. A SWAT team, an ambulance, and a fire engine responded to the Rite Aid, and officers closed off the parking lot as a precaution. A Salt Lake Police detective said the incident started when the man entered the store carrying a clear

container filled with gasoline and a rag hanging out of the top. He made his way toward the pharmacy and somehow got back by the medications. Employees and customers called for help and were evacuated from the building as police responded.
Source: http://www.sltrib.com/sltrib/news/53376009-78/police-pharmacy-lake-salt.html.csp

42. *January 25, Associated Press* – (California) **Odor causes evacuation of Universal Studios office.** Firefighters in Los Angeles County, California, evacuated more than 400 people from a high-rise building at Universal Studios January 25 after reports of a possible refrigeration gas leak. The fire inspector said reports of a chlorine gas smell prompted the evacuation of a 15-story building housing studio executive offices. About 100 firefighters and a hazardous materials unit were at the scene. The fire inspector said there was no gas cloud.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/01/25/state/n134720S55.DTL

43. *January 25, KLEW 3 Lewiston* – (Idaho) **Moscow apartment explosion explained.** Moscow fire officials said they believe they have uncovered the cause of the gas explosion that occurred at a Moscow, Idaho apartment complex the week of January 16. â□¨Fire marshals said an undetected fire in the attic of the Elysian apartments was the cause of the explosion, which damaged the entire building and left tenants without a home, KLEW 3 Lewiston reported January 25. Officials said the combination of heat, smoke, and carbon monoxide gas coupled with the attic's insulation created conditions that produced the explosion. Fire pattern analysis led investigators to the utility chase and furnace as the point-of-origin of the fire, which severely damaged the building. "There's a chance that the building might come down and be rebuilt, there's a chance that portions of the building will be re-built," the Moscow fire chief said.
Source: http://www.klewtv.com/news/local/Moscow-apartment-explosion-explained--138084048.html

44. *January 25, Redding Record Searchlight* – (California) **Police: Bomb found and removed at Red Bluff parking lot.** Officers with the Red Bluff, California Police Department called in the bomb squad after they found homemade explosives in a parking lot January 25. Officers said they arrived at the Riverside Plaza after onlookers reported a suspicious package. After evacuating people from the area, officers said they cordoned off the parking lot for 2 hours after discovering 6-inch pipe bombs with fuses attached. Two officers from the Shasta County Bomb Squad arrived and transported the bombs to a rural location where they were detonated.
Source: http://www.redding.com/news/2012/jan/25/police-bomb-found-and-removed-red-bluff-parking-lo/

45. *January 25, Boston Globe* – (Massachusetts) **150 elderly residents evacuated after two-alarm blaze hits Melrose housing complex.** Almost 150 elderly residents were evacuated on Massachusetts Bay Transportation Area (MBTA) buses and taken to nearby hotels after a mattress caught fire in a Melrose housing complex January 25. Police said the two-alarm fire broke out in an apartment on the fourth floor of the 8-

story Julian Steele House. According to the police report, it was caused by the "careless disposal of smoking material." The fire was confined to a mattress and box spring, police said, but due to the sprinkler system going off, the building sustained heavy water damage. The water from the sprinklers spread throughout the building and posed an electrical hazard, a fire captain said. Police estimated damage at more than $100,000. The 140 residents were transported via MBTA buses to hotels, where they were scheduled to reside until January 26 or 27.
Source: http://www.boston.com/Boston/metrodesk/2012/01/elderly-residents-evacuated-after-two-alarm-blaze-hits-melrose-housing-complex/AKHt3GQiOqE8S7IisHHukN/index.html

46. *January 25, Huntsville Times* – (Alabama; National) **Tide fans ordering from Bamastuff.com may have had credit card information stolen.** University of Alabama fans who bought items from Bamastuff.com between August 1, 2009, and January 16, 2012, are being alerted to contact their banks for possible illegal and unauthorized use of their credit cards, the Huntsville Times reported January 25. Bamastuff.com has sent out e-mail notifications informing customers about a breach in its database, which was discovered the week of January 23 by the company's information technology (IT) director. In his e-mail, the IT director said information including customers' names, e-mail addresses, billing and shipping addresses, telephone numbers, credit card information, and/or cryptographically scrambled passwords could have been stolen. In a phone interview with the Huntsville Times, he said he knows of numerous fraudulent charges made on Bamastuff.com customers' bank accounts. "We are still investigating the server's log files to pinpoint exactly what was taken and how," he wrote. The e-mail included the expiration date of the card used so customers will know which card was used, although most are likely past their expiration date, he said. He said they are fairly certain that orders placed after January 16 are not affected based on the access logs on the server. "It appears to be a one time attack and we have taken numerous steps to fend off any future ones," he said. He also said old orders, including names, addresses and credit card numbers, are being archived and customer data is being deleted from the system for those not placing an order with Bamastuff.com since the start of the 2009 season. To protect against future theft, he said the company has upgraded and installed various security software to monitor activity.
Source: http://blog.al.com/breaking/2012/01/tide_fans_ordering_from_bamast.html

For more stories, see items **21** and **39**

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

47. *January 26, Towanda Daily Review* – (Pennsylvania) **Athens receives grant to repair levee.** The Commonwealth Financing Authority board January 25 approved a grant for $452,000 in H2O PA Flood Control funds to Athens Borough, Pennsylvania. The funds will cover the borough's portion of a project to rehabilitate a 400-foot section of the Chemung River levee substantially damaged in the September flooding caused by Tropical Storm Lee. As part of the borough's agreement with the U.S. Army Corps of Engineers, who will perform the repairs, the borough is responsible for 20 percent of the project's total cost. Temporary repairs were made to the levee in October.
Source: http://thedailyreview.com/news/athens-receives-grant-to-repair-levee-1.1262858

48. *January 25, Cache Valley Daily* – (Utah) **Mendon assesses damage caused by flooding.** After a several days of concentrated precipitation the week of January 16, the Mendon, Utah, area of Cache Valley experienced damaging effects of flooding that are now being assessed and remedied, the Cache Valley Daily reported January 25. Repairs will be made in the spring, but the cost is unknown the Mendon Fire and Rescue chief said. State Road 23 from Mendon to Wellsville was closed to traffic for 2 days due to the canal flowing over the road, pushing water and mud debris into drivers' paths. Crews purposely breached the canal to prevent it from breaching itself with more devastating effects. The water was allowed to flow across SR 23 on a premeditated course. Officials estimated crews and volunteers put out about 4,000 sandbags that helped prevent further damage.
Source: http://www.cachevalleydaily.com/news/local/Mendon-assseses--138061703.html

For another story, see item 7

[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