



Homeland Security

Daily Open Source Infrastructure Report for 21 January 2011

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- Nine schools in the Woodland Hills area of Los Angeles, California, were locked down for hours after a school police officer was shot near a campus January 19, according to the Associated Press. (See item [36](#))
- KGO 7 San Francisco reports police arrested a woman for storing five pipe bombs, including at least one with glass shards, in a storage locker in Pacheco, California. (See item [50](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)
- [National Monuments and Icons](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - <http://www.esisac.com>]

1. *January 20, Sikeston Standard Democrat* – (Missouri) **Coal train derails in Sikeston.** Burlington Northern Santa Fe railroad employees worked January 18 to clear the damage from a train derailment that occurred in Sikeston, Missouri. At 4:49 p.m., the derailment of a southbound coal train en route to the Sikeston Power Plant was reported to the Sikeston Department of Public Safety (DPS). Six cargo cars were affected in the derailment — one was completely on its side, another was tilting, while

two cars were completely off the track and two were partially off the track, said DPS captain. A stretch of Wakefield Avenue between Davis Boulevard and Northwest Street was closed for a short time, but reopened around 7 p.m., according to the captain. Northwest Street remained closed until just after 9:30 p.m. near the crossing as railroad employees worked to clean up the mess. Also closed for the time being were the north-south rails. The captain said there were no injuries, and the damage was confined to the railroad tracks and cars. The cause of the derailment was unknown.

Source: <http://www.semissourian.com/story/1696333.html>

2. *January 20, U.S. Consumer Product Safety Commission* – (National) **Aux Sable liquid products recalls to inspect propane gas; can pose fire and burn hazards.** The U.S. Consumer Product Safety Commission, in cooperation with Aux Sable Liquid Products, announced a voluntary recall of propane gas sold in portable cylinders and delivered to storage tanks January 20. The recall involves odorized propane gas delivered for storage tanks or sold in portable cylinders between February 25, 2010 and September 30, 2010. Some of this propane does not have sufficient levels of the odorant that is added to propane to help alert consumers to a gas leak. Failure to detect leaking gas can present fire, explosion and thermal burn hazards to consumers. The amount of propane being recalled equates to 700 rail cars full. So far, no injuries have been reported. The propane was sold and distributed through propane retailers in the following states: Connecticut, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, North Carolina, Pennsylvania, Rhode Island, Tennessee, Vermont, and Virginia. Customers in the affected states should contact Aux Sable immediately to arrange for a free inspection.

Source: <http://www.cpsc.gov/cpsc/pub/prerel/prhtml11/11102.html?tab=recalls>

3. *January 19, Associated Press* – (West Virginia) **Feds blame gas, dust for deadly W.Va. mine blast.** A small methane gas fire that was not doused because of broken equipment sparked a massive coal dust explosion last April that killed 29 miners at Massey Energy Co.'s Upper Big Branch mine, the U.S. Mine Safety and Health Administration (MSHA) said January 19. Massey records and evidence found deep inside the West Virginia mine points to poor maintenance in the deadliest U.S. coal mine explosion since 1970, MSHA officials told reporters during a conference call. The agency expects to finish its probe in a few months, but said it wanted to issue preliminary findings. Those findings include worn and broken equipment investigators believe contributed to the initial fire and made it impossible to put out, and poor housekeeping that allowed excessive amounts of explosive coal dust to coat much of the mine just before the blast. Investigators believe the explosion started when badly worn teeth on a 1000-foot-wide mining machine created a spark that ignited as little as 13 cubic feet of methane. Tests that Massey resisted showed some of the machine's 48 water sprayers for controlling dust and dousing sparks were not working at the time. When the flames ignited coal dust, it unleashed a blast that killed everyone, including co-workers more than 1 mile away. Investigators are still trying to determine whether the mine's ventilation system was working properly at the time.

Source: <http://www.businessweek.com/ap/financialnews/D9KRJU200.htm>

4. *January 19, Bloomberg* – (North Dakota) **Tesoro has fire in gasoline unit at Mandan refinery.** Tesoro Corp. is assessing the damage from a fire in a gasoline-making unit at its Mandan, North Dakota, oil refinery, a company spokesman said. The blaze, which started January 19 was put out at about 3:30 p.m., he said. The spokesman said all workers were accounted for, and that the refinery is running at a reduced rate. The fire occurred on the north side of the property at an oil furnace, the Morton County emergency manager said. Flow to the oil furnace was stopped. The refinery processes primarily sweet domestic crude oil from North Dakota, the company spokesman said. The 58,000-barrel-per-day plant, built in 1954, manufactures gasoline, diesel fuel, jet fuel, heavy fuel oils, and LPG, he said. Refined products are trucked and shipped by train from Mandan and shipped via pipeline to supply the Jamestown, North Dakota, area, as well as eastern North Dakota and Minnesota.
Source: <http://www.businessweek.com/news/2011-01-19/tesoro-has-fire-in-gasoline-unit-at-mandan-refinery.html>

[\[Return to top\]](#)

Chemical Industry Sector

5. *January 20, Associated Press* – (West Virginia) **Report says workers made mistakes before WV plant explosion.** Federal investigators said Bayer CropScience workers made critical mistakes as they rushed to restart a pesticide manufacturing unit, leading to an explosion that killed two workers in August 2008 in West Virginia. The U.S. Chemical Safety Board reached that conclusion in a report issued January 20. Investigators said Bayer deviated from written start-up procedures before the explosion blasted apart a tank filled with toxic chemicals. One worker died in the blast, which packed the punch of 17 sticks of dynamite and caused damage 7 miles away. A second died weeks later from burns. The board said investigators also found Bayer bypassed safety devices and conducted an inadequate safety review. In a response, Bayer said safety remains its highest priority. The Bayer vice president planned to participate in a public meeting on the accident January 20 at West Virginia State University. He said Bayer has already implemented significant safety measures that include improvements in communications, training, monitoring, supervision, and equipment.
Source:
http://www.whsv.com/westvirginiaap/headlines/Report_Says_Workers_Made_Mistake_s_Before_WV_Plant_Explosion_114286684.html
6. *January 19, Redding Record-Searchlight* – (California) **I-5 reopened after chemical truck fire closure north of Redding.** A toxic plume of smoke from a truck burning near Interstate 5 in California forced officials to close the freeway for about an hour January 19. A California Highway Patrol (CHP) officer said residents called 911 at about 1:30 p.m. to report an explosion in the area of the Fawndale exit on I-5, about 10 miles north of Redding. A truck with a hopper containing gravel and a tank containing polyurethane had caught fire. The truck was parked in an equipment yard adjacent to the freeway. The fire was burning the polyurethane and putting up a plume of smoke that could irritate the lungs and skin, the Mountain Gate Fire Department chief said.

The CHP officer said the freeway was closed to prevent freeway travelers from being exposed to the smoke. The freeway was closed northbound at Wonderland Boulevard and southbound at Bridge Bay, a spokeswoman from the California Department of Transportation said. CHP reopened the freeway in both directions shortly before 2:30 p.m. A Mountain Gate engine was the first at the fire and it took about 35 minutes to stop the flames. At least two Mountain Gate engines and a tanker responded to the fire. The California Department of Forestry and Fire Protection responded to the fire with four engines and one water tender.

Source: <http://www.redding.com/news/2011/jan/19/truck-fire-reported-i-5-north-redding/>

For more stories, see items [30](#) and [31](#)

[\[Return to top\]](#)

Nuclear Reactors, Materials and Waste Sector

7. *January 19, Global Security Newswire* – (International) **Radioactive capsules recovered in India.** Indian authorities have recovered four radioactive isotope cylinders and detained one person allegedly linked to the apparent theft of the material, the Statesman reported January 15. The capsules turned up inside a public restroom at a low-income neighborhood near the Durgapur Steel Plant, the site of their disappearance. The removal of the capsules prompted concerns among managers, police, and experts about the facility’s security measures. The site is continuously overseen by 1,500 personnel with India’s Central Industrial Security Force. The capsules are “deadly harmful for human beings and are supposed to be preserved in a secure environment,” plant officials said. Experts have expressed concern radioactive material could be dispersed by a radiological “dirty bomb.”
Source: http://www.globalsecuritynewswire.org/gsn/nw_20110119_7551.php
8. *January 18, Computerworld* – (National) **Gaping security flaw exposed on anti-tamper devices.** Security devices used in transportation, packaging, and even in accounting for nuclear materials are very vulnerable to attack, two security researchers warned January 18 at a Black Hat security conference in Arlington, Virginia. The physical security devices, known as “tamper-evident devices,” are not intended to prevent theft but to alert inspectors something has been broken into. The devices are wide-ranging in design and application, and are used to seal everything from evidence bags, large shipping containers and even things like the warranty seal on gaming consoles. Two analysts with i11 Industries went through a long list of tamper-evident devices at the conference and explained, step-by-step, how each seal can be circumvented with common items, such as solvents, hypodermic needles, razors, blow dryers, and in more difficult cases with the help of tools such as drills. The more difficult devices may be bolt locks designed to secure shipping containers, or polycarbonate locks designed to shatter if cut.
Source:

http://www.computerworld.com/s/article/9205461/Gaping_security_flaw_exposed_on_anti_tamper_devices

[\[Return to top\]](#)

Critical Manufacturing Sector

9. *January 20, Pittsburgh Post-Gazette* – (Pennsylvania) **OSHA lists violations against plant where workers died.** The Occupational Safety and Health Administration (OSHA) issued a laundry list of violations against a Monaca, Pennsylvania-based chemical plant following an investigation into an explosion that resulted in the death of two employees there July 23, 2010. The agency proposed a total of \$45,000 in fines for the Horsehead Corp. for nine violations — eight of them classified as “serious.” The company runs a zinc refinery. Among other things, OSHA found that the company created unsafe working conditions by putting employees directly in harm’s way in the event of an explosion.
Source: <http://www.post-gazette.com/pg/11020/1119246-57.stm>

10. *January 19, Computerworld* – (International) **Keyless systems on cars easily hacked, researchers say.** The passive keyless entry and start systems supported by many modern cars are susceptible to attacks that allow thieves to relatively easily steal the vehicles, security researchers at Switzerland’s ETH Zurich University said. In demonstrations using 10 cars from 8 makers, the researchers showed how they were able to unlock, start and drive away the cars in each case, by outsmarting the smart key system. The break-ins were carried out using commercial, off-the-shelf electronic equipment available for as little as \$100, the researchers said in a paper describing their exploits. Although the possibility of such attacks on keyless systems has been discussed previously, it has not been clear before if they would be feasible on modern cars, the researchers said. “In this paper, we demonstrate that these attacks are both feasible and practical,” they said.
Source:
http://www.computerworld.com/s/article/9205478/Keyless_systems_on_cars_easily_hacked_researchers_say

[\[Return to top\]](#)

Defense Industrial Base Sector

11. *January 20, DefenseNews* – (International) **Part of Airbus tanker’s refueling boom falls off during exercise.** A substantial part of the in-flight refueling boom onboard an Airbus A330 MRTT tanker destined for the Royal Australian Air Force has broken off and fallen into the Atlantic Ocean during an exercise. The major part of the boom broke off part-way through refueling a Portuguese Air Force F-16 at around 5 p.m. January 19, an Airbus Military spokesman said. Both aircraft returned to their respective bases with minor damage. The spokesman said it was the 14th refueling contact of the exercise. He said it was too early to say whether technical, human, or other factors

caused the boom to break off. The boom was designed by the European Aeronautic Defence and Space Company N.V., and has yet to enter service with any air force. The system is the same one being offered to the U.S. Air Force in the tanker competition underway against rival bidder Boeing.

Source: <http://www.defensenews.com/story.php?i=5498719&c=EUR&s=AIR>

12. *January 20, WTAM 1100 Cleveland* – (Ohio) **Major fire hits Ashland.** Firefighters responded to a big blaze that erupted just before 10:30 p.m. January 19 at Philway Products on Virginia Avenue in Ashland, Ohio. Philway manufactures printed circuit boards for military and commercial use. It took many fire departments to get the blaze under control, and the neighborhood was evacuated due to the initial threat of chemicals stored in the affected area. The EMA director said homes near the plant were evacuated as a precaution with residents moved to a community center. The factory has 40 employees, but it is believed no one was in the building at the time of the fire. The blaze did not end up reaching the chemicals and the fire was brought under control, but in the early morning of January 20, there was still heavy smoke in the area, with officials advising motorists to use caution. Firefighters from Ashland, Mansfield, Jeromesville, Savannah, and Polk-Jackson-Perry fire departments responded to the blaze.

Source: <http://www.wtam.com/cc-common/news/sections/newsarticle.html?feed=122520&article=8067056>

[\[Return to top\]](#)

Banking and Finance Sector

13. *January 20, New York Times* – (International) **Theft of E.U. emission permits estimated at \$37.7 million.** European Union (EU) regulators said January 20 that the value of greenhouse gas emission permits stolen in online attacks over recent days was about 28 million euros, and that employees of companies connected to the system might have played a role in the thefts. The European Commission shut down its Emissions Trading System, its main tool to control greenhouse gas emissions, January 19 to stop the spate of thefts, valued at the equivalent of \$37.7 million. The commission, the E.U.'s executive arm, initially put most of the blame on computer hackers and on poor computer security. An E.U. official said some companies that regularly use the system admitted their employees could be "implicated" in the thefts. The thefts were carried out at electronic registries in Austria, Greece, the Czech Republic, Poland, and Estonia, according to the commission. The commission said spot trading at all E.U. registries, which track ownership of allowances, would be suspended until at least January 26.

Source: <http://www.nytimes.com/2011/01/21/business/global/21carbon.html>

14. *January 20, IDG News Service* – (International) **Fraudster's money mules in short supply, says Cisco.** A new security report from Cisco Systems estimated the amount of stolen online bank account data far exceeds the number of people fraudsters can get to transfer stolen funds, who are known as "money mules." A mule is someone who either

knowingly helps or is tricked into moving money from a victim's bank account through their own account and then onto a third party, usually located in another country. Money is transferred from the victim's account to the mule's account, and the mule is then instructed to quickly withdraw the money and do a wire transfer or an ACH (Automated Clearing House) transfer. The ACH system is used by financial institutions for exchanging details of direct deposits, checks, and cash transfers made by businesses and individuals. Despite increasing awareness of the schemes, often advertised as "work-at-home" jobs with generous salaries, many people still get caught up in the frauds. Cisco said in its 2010 Annual Security Report that the ratio of stolen account credentials — which can be acquired through phishing or hacking — to available mule capacity could be as high as 10,000 to 1.

Source:

http://www.computerworld.com/s/article/9205625/Fraudster_s_money_mules_in_short_supply_says_Cisco

15. *January 19, Internet Crime Complaint Center* – (National) **E-mails containing malware sent to businesses concerning their online job postings.** Recent FBI analysis revealed cyber criminals engaging in ACH/wire transfer fraud have targeted businesses by responding via e-mail to employment opportunities posted online. Recently, more than \$150,000 was stolen from a U.S. business via unauthorized wire transfer as a result of an e-mail the business received that contained malware. The malware was embedded in an e-mail response to a job posting the business placed on an employment Web site and allowed the attacker to obtain the online banking credentials of the person authorized to conduct financial transactions within the company. The malicious actor changed the account settings to allow the sending of wire transfers, one to the Ukraine, and two to domestic accounts. The malware was identified as a Bredolab variant, svrWSC.exe. This malware was connected to the Zeus/Zbot Trojan, which is commonly used by cyber criminals to defraud U.S. businesses.
Source: <http://www.ic3.gov/media/2011/110119.aspx>

16. *January 19, Asbury Park Press* – (New Jersey) **Highlands man charged in bomb threat at Rumson bank.** A Highlands, New Jersey man threatened to blow up a borough bank as he was leaving it January 18, prompting a lockdown and a call for the New Jersey State Police Bomb Squad, officials said. The 63-year-old suspect — from Portland Road — shouted "I will blow this (expletive) bank up" as he and another man left the Bank of America branch on West River Road around 4:20 p.m., according to Monmouth County's administrative assistant prosecutor. Rumson police arrived on scene after a bank employee alerted them to the threat and found the men in a car in the parking lot. Both men were detained, and the suspect was later charged with third-degree making terrorist threats and causing false public alarm, the assistant prosecutor said. The second man has not been charged with any offenses.
Source: <http://www.app.com/article/20110119/NEWS/110119108/Highlands-man-charged-in-bomb-threat-at-Rumson-bank>

17. *January 18, WJW 8 Cleveland* – (Ohio) **8 arrested in identity theft ring ran from federal prison.** Eight individuals from the Cleveland, Ohio, area have plead guilty to their roles in an identity-theft ring ran by a man locked up in a federal prison. According to officials with the office of the U.S. Attorney, Northern District of Ohio, a 34-year-old suspect, who resides in Atlanta, Georgia, was sentenced to 14 additional years in prison January 18 for running the identity theft ring out of Fort Dix Federal Correctional Institution. He ran the scheme from August 2009 to April 2010. Federal prosecutors said the suspect was able to get personal information communicated to him while in the prison, including names, addresses, and Social Security numbers of credit card holders at various department stores. He would then contact the stores and add additional users to the accounts or open new accounts in the person's name. Prosecutors said the suspect then communicated with his co-conspirators, all eight of whom lived in the Cleveland area, and the cards were used to purchase \$254,000 in merchandise.
Source: <http://www.fox8.com/news/wjw-news-eight-cleveland-arrests-identity-thefts,0,7030183.story>

18. *January 18, KTRK 13 Houston* – (National) **Four suspected in sophisticated ID theft ring.** Police are searching for four suspects accused of operating a massive identity theft ring. They said it is a far reaching investigation, with victims across the United States. Police said the suspects are still at large. So far, they have identified at least 28 victims from Houston, Richmond, and Cypress, Texas, and even as far away as California. Police said surveillance video shows a male suspect purchasing gift cards more than 1 year ago. Investigators said he orchestrated the ID theft, along with his girlfriend, her brother, and her daughter. Detectives said they lived in two homes in Pearland, Texas, where police reportedly found \$30,000 in cash last July. Detectives said the suspects had an accomplice, likely a cashier at another business who skimmed legitimate credit card data from unsuspecting customers. The suspects would then allegedly transfer that information to the magnetic strips on the back of blank cards and then emboss the cards with their own names and bogus numbers. The credit cards were then used to purchase gift cards, repeatedly. Police said the cards were either used by the suspects or sold. The male suspect was arrested in July, but bonded out and has since disappeared. Police believe he and the other three suspects are still somewhere in the Houston, Texas, area.
Source: <http://abclocal.go.com/ktrk/story?section=news/local&id=7905020>

For another story, see item [41](#)

[\[Return to top\]](#)

Transportation Sector

19. *January 20, Seer Press News* – (Washington) **Two Amtrak Pacific Northwest routes closed after mudslides.** Amtrak's Seattle to Vancouver Cascades line and the Empire Builder route to Chicago's Seattle-Everett leg were closed January 19 due to heavy rains and mudslides in Washington State. According to reports, the passengers who

regularly rode the trains traveling on the said tracks were offered bus rides to their destinations instead. The Burlington Northern Santa Fe (BNSF) Railway, which operates the two lines, has issued the restriction which will last until January 21, according to Reuters. A BNSF spokesman told Reuters that heavy rains and thawing of snow caused mudslides along many parts of the 155-mile Cascades line, which is the 35-mile Seattle-Everett part of the Empire Builder route. According to Reuters, BNSF tracks have been hit by two mudslides near Everett and Mukilte.

Source: <http://seerpress.com/two-amtrak-pacific-northwest-routes-closed-after-mudslides/23025/>

20. *January 19, WPLG 10 Miami* – (Florida) **Police arrest ‘suspicious’ man at airport.** A man was arrested and turned over to federal authorities January 18 after police said he was taking photos of “sensitive areas” inside and outside of a terminal at Miami International Airport in Miami, Florida. According to the incident report from Miami-Dade County police, the 32-year-old suspect was seen walking through the airport and taking pictures January 11. A sergeant stopped the suspect in the Dolphin parking garage. Police said the suspect did not give them any information about what he was doing or why. In the incident report, the sergeant described his behavior as “evasive.” Police said there was no indication the suspect had a plane ticket. After further investigation, federal immigration authorities said the suspect was in the country illegally and wanted for violating U.S. immigration law. Because Miami International Airport is a public facility, anyone is allowed to take video and pictures inside. An official from the Transportation Security Administration (TSA) told Local 10 that if photography is stepping over the line into surveillance, TSA agents should alert police. Source: <http://www.justnews.com/news/26535234/detail.html>

21. *January 19, Homeland Security Today* – (National) **Tech limitations could allow illegal entries by seafaring workers: GAO.** Foreign workers with criminal or terrorist connections onboard sea vessels could elude detection by the Department of Homeland Security (DHS) because U.S. Customs and Border Protection (CBP) lacks the capability to electronically verify their admissibility to the United States using mobile technology at U.S. ports, congressional investigators warned January 18. CBP and the U.S. Coast Guard, along with the State Department, hold responsibility for screening seafaring workers traveling onboard boats to make certain they are not security risks, the Government Accountability Office (GAO) said in *Maritime Security: Federal Agencies Have Taken Actions to Address Risks Posed by Seafarers, but Efforts Can Be Strengthened*. The State Department screens seafaring workers who apply for non-immigrant U.S. visas overseas, while DHS agencies screen seafarer manifests and inspect the admissibility of individual workers arriving at U.S. seaports. But, the GAO report observed, “CBP conducts cargo vessel admissibility inspections on board the vessel without the benefit of tools to electronically verify a seafarer’s identity or immigration status because of a lack of available connectivity to network communications in the maritime environment. DHS has prioritized the acquisition of a mobile version of this technology capability, but expects it to take several years before the technology is developed and available.” Without mobile identity verification technology, CBP faces increases risk of foreign seafarers opting to become illegal

immigrants in the United States, the report concluded. CBP has not formally conducted an assessment of risks associated with the lack in mobile verification capability.

Source: <http://www.hstoday.us/briefings/daily-news-briefings/single-article/tech-limitations-could-allow-illegal-entries-by-seafaring-workers-gao/93a451c5db980d6842f229c320bab227.html>

For more stories, see items [1](#), [6](#), and [23](#)

[\[Return to top\]](#)

Postal and Shipping Sector

22. *January 20, Schenectady Daily Gazette* – (New York) **State police bomb squad called to remove suspicious tank in Schenectady.** A rusty old propane tank forced the closure of the post office and country public library in Schenectady, New York, January 20 as emergency officials investigated it a potential bomb threat — a day before a visit by the U.S. President. A passer-by flagged down a city bureau of services truck at about 8:15 a.m. to let them know of the tank sitting on the side of the road on Clinton Street by the post office’s delivery entrance, a Schenectady police spokesman said. Customers were evacuated from the post office and people looking to use the library, which opens at 9 a.m., were prohibited from entering. Officers set up a perimeter around the suspicious object, blocking off Clinton Street and then later Liberty Street from Jay Street to Lafayette Street as they waited for the New York State Police Bomb Squad Unit to arrive. The 18 postal employees remained inside as police investigated and were evacuated at about 10:15 a.m., according to the Schenectady postmaster. A state police bomb-sniffing dog searched around the perimeter of the post office for any explosive materials and found none. The propane tank was empty. The scene was clear by about 10:15 a.m.

Source: http://www.dailygazette.com/news/2011/jan/20/12011_tank/

23. *January 20, New Haven Post-Chronicle* – (Connecticut) **Amtrak train, Fed Ex truck collide in Wallingford.** An Amtrak train in Wallingford, Connecticut, hit a FedEx tractor-trailer laden with packages January 18, sending “letters and paper flying everywhere,” according to a witness. The crash at 7:22 a.m. occurred when the truck had engine trouble and got stuck on the track at a railroad crossing on Toelles Road near Route 5. Because the train was traveling at what a fire captain said was “a low rate of speed,” there were no injuries to the truck driver or any of the 98 people on the train. The train was southbound, headed for New Haven’s Union Station, and “had slowed almost to a stop” as it neared the truck, which was on the tracks. “The train only went about 20 feet down the track after it went through the truck,” the fire captain said. The train was pulling at least a half-dozen cars behind the locomotive. A spokesman for Amtrak said the train, No. 141, was part of the Springfield, Massachusetts, shuttle service. The train was removed from the scene at 11:38 a.m., and service along the New Haven to Springfield corridor returned to normal a short time later, an Amtrak spokeswoman said January 18.

Source:

<http://www.ctpostchronicle.com/articles/2011/01/20/news/doc4d35b3422da2d544013412.txt>

[[Return to top](#)]

Agriculture and Food Sector

24. *January 20, Fort Wayne Journal Gazette* – (Indiana) **52 counties are disaster areas.** Fifty-two counties in Indiana were recently declared disaster areas from the drought that lasted from August 1 through December 31. The U.S. Department of Agriculture (USDA) issued the declaration as a result of losses to the agricultural industry. “This action will provide help to hundreds of farmers who suffered significant production losses,” the U.S. Agriculture Secretary said in a prepared statement. Farmers in Allen, DeKalb, Huntington, Kosciusko, Noble, Steuben, Wells, and Whitley counties are eligible for natural-disaster relief through low-interest emergency loans from the USDA’s Farm Service Agency.
Source: <http://www.journalgazette.net/article/20110120/LOCAL/301209924/1002/LOCAL>

25. *January 20, Food Safety News* – (Hawaii) **Botulism fear prompts recall of black bean sauce.** Hawaii Business Group Inc., Barb’s Favorite Recipes, and Ohana Seafoods are recalling Barb’s Local Style Black Bean Sauce and Ohana Flavors Black Bean Sauce because of possible health risks due to the potential growth of Clostridium Botulinum (botulism), a bacterium which can cause life-threatening illness or death. The sauce was manufactured by First Commercial Kitchen LLC. The Black Bean Sauce is sold in 12-ounce glass jars and labeled as Barb’s Local Style Black Bean Sauce or Ohana Flavors Black Bean Sauce. The UPC numbers on the product are 6-75981-42491-8 and 7-02003-72739-6. The recalled sauce was distributed on Oahu and Molokai. A routine inspection discovered the problem.
Source: <http://www.foodsafetynews.com/2011/01/botulism-fears-prompt-recall-of-black-bean-sauce/>

26. *January 20, Food Safety News* – (New York) **Improperly pasteurized milk recalled in New York.** New York State’s acting agriculture commissioner alerted consumers January 20 that certain milk products distributed by FingerLakes Farms LLC, from Plant #36-1131, are being voluntarily recalled due to improper pasteurization. Proper pasteurization heats milk in order to effectively eliminate all pathogenic bacteria, such as Listeria and Salmonella. The recalled milk products are sold under the names Ithaca Milk Company Lowfat Milk, and Ithaca Milk Company Cream on Top Whole Milk. Both of these milk products were packaged in quart, half-gallon, and gallon sizes of plastic containers. All of the products have a container code of SELL BY 013111 and were distributed in the Buffalo, Rochester, Syracuse, and Finger Lakes regions. Routine sampling by New York State Department of Agriculture and Markets Milk Control and Dairy Services inspectors, and subsequent analysis of the product by New York State Food Laboratory personnel, revealed the product was improperly pasteurized.
Source: <http://www.foodsafetynews.com/2011/01/milk-recalled-in-new-york/>

27. *January 19, Salem Statesman Journal* – (Oregon) **Imported bug found in Polk County.** The Oregon Department of Agriculture has confirmed a single detection of light brown apple moth, marking the first time the pest has been found in the state. There is no evidence a breeding population of the moth exists in Oregon. The insect — a native of Australia that harms fruit orchards — likely came in with imported nursery stock, state officials said. The single moth was found in the summer of 2010 in a trap at a Polk County nursery. State officials said the identification of exotic moths can take months, and the suspect specimen was recently confirmed. In 2010, the state agriculture department placed 1,000 traps for the moth throughout the state. No other moths were caught in Oregon. In 2007, the light brown apple moth was first detected in the continental United States when it was found in California’s Bay Area. The pest has been established in Hawaii.
Source: <http://www.statesmanjournal.com/article/20110119/UPDATE/110119042/-1/update>
28. *January 19, Associated Press* – (Georgia) **Fire extinguished at Ga. sugar refinery.** Firefighters said they quickly extinguished a fire at the Imperial Sugar refinery near Savannah, Georgia. Port Wentworth’s fire chief said all employees evacuated safely January 19 when construction workers’ power tools started a fire on the roof of the refinery’s packing plant. Officials said the fire was contained in about 5 minutes.
Source: <http://www.wrcbtv.com/Global/story.asp?S=13870905>
29. *January 19, Food Safety News* – (National) **Chicago ground beef recall expanded.** Columbus Meat, a Chicago, Illinois, company, has expanded a food recall to include an additional 580 pounds of ground beef patties that may be contaminated with E. coli 0157:H7. Columbus Meat took the action after state inspectors discovered the same batch of contaminated source material was used to produce patties on more than one day. As a result, patties with lot numbers 361361, 361362 and 361364 that were produced on December 29-31 and January 3 have been added to the recall, which also includes 200 pounds of ground beef made December 27. The labels on each package of suspect patties bear an inspection legend shaped like the state of Illinois that contains the establishment number “775.” It is believed the patties were distributed in the Chicago area to food-handling establishments such as restaurants and grocery stores.
Source: <http://www.foodsafetynews.com/2011/01/chicago-ground-beef-recall-expanded/>

[\[Return to top\]](#)

Water Sector

30. *January 20, Associated Press* – (New Hampshire) **Mass. company pleads to NH ammonia contamination.** A Massachusetts refrigeration company is facing a fine of up to \$500,000 after it pleaded guilty to a federal charge it contaminated a New Hampshire wastewater facility by pouring ammonia down a drain. American

Refrigeration Co. of Andover, Massachusetts, has pleaded guilty to a charge a technician poured ammonia into a drain January 24, 2008, knowing it led to the Suncook Wastewater Treatment Facility. Federal prosecutors said the ammonia killed organic materials used to treat wastewater, and as a result the facility dumped untreated or significantly under-treated wastewater into the Merrimack River. The Concord Monitor said it took 4 days for the plant to return to normal operations.

Source:

http://www.boston.com/news/local/new_hampshire/articles/2011/01/20/mass_company_pleads_to_nh_ammonia_contamination/

31. *January 20, Philadelphia Inquirer* – (Pennsylvania) **Chemical company charged with pollution.** The U.S. attorney's office January 19 charged a Marcus Hook, Pennsylvania chemical company with violating the Clean Water Act for discharging tainted water into the Marcus Hook Creek, a tributary to the Delaware. Employees of Chemical Equipment Labs Inc., on Walnut Street in Philadelphia, Pennsylvania, routinely rinsed plastic containers that had previously held chemicals, then discharged the wastewater into a drain in a bathroom that led to the sewer system, according to a federal criminal complaint. The company sells and distributes chemicals, including pool chemicals, ice-melting products, and oil absorbents. The charges stem from an incident on April 25, 2007. Employees allegedly washed the inside of a truck tank that had previously contained chlorine, according to the complaint. Liquid from a valve on the truck, which sat in a loading bay in front of the facility, pooled and then washed into a manhole in the parking lot. The wastewater then flowed into the creek, about 600 feet away. The next day, police and firefighters responded to a report of a chemical spill into the Marcus Hook Creek that altered the stream's pH level. Officials traced samples to the truck valve and blamed the leak for increasing the stream's pH to a range of 9 to 10.2. If convicted, the company could be placed on probation for up to 5 years and fined up to \$200,000.

Source:

http://www.philly.com/inquirer/local/pa/20110120_Chemical_company_charged_with_pollution.html

32. *January 19, United Press International* – (California; International) **Mexican sewage pollutes Calif. beaches.** Millions of gallons of raw sewage are flowing down Mexico's Tijuana River to the Pacific Ocean, prompting the closure of San Diego, California-area beaches, officials said. The Baja California, Mexico, Health Department said the 30-inch-diameter pipe linking a pump station to the Punta Bandera treatment plant broke about a mile south of the U.S. border during December's rainstorms. Estimates of the size of the spill vary from 1.3 million gallons to 30 million gallons per day, and will be among the largest single incidents in the last 10 years to affect San Diego County, the San Diego Union-Tribune reported January 18. The issue of wastewater has caused tension along the U.S.-Mexican border for the last 70 years because Tijuana's sewage system has not kept up with modern methods. U.S. and Mexican agencies have tried to minimize the pollution by constructing treatment plants and other facilities, the Union-Tribune reported.

Source: http://www.upi.com/Top_News/US/2011/01/19/Mexican-sewage-pollutes-Calif-beaches/UPI-64391295479373/

[\[Return to top\]](#)

Public Health and Healthcare Sector

33. *January 19, Associated Press* – (Vermont) **Vermont AG settles data breach case for \$55,000.** The Vermont attorney general’s office said a Connecticut-based health insurance company is ready to pay \$55,000 to settle a complaint it did not inform customers that personal information had been lost along with an unencrypted computer hard drive. The state said the complaint and proposed settlement with Health Net Inc. and Health Net of the Northeast Inc. of Shelton, Connecticut, were both filed January 14. The case arose after the loss of a portable hard drive that contained protected health information, Social Security numbers, and financial information of about 1.5 million people, including 525 Vermonters. Health Net discovered the drive was missing May 14, 2009 but did not start notifying affected Vermont residents until more than 6 month later.

Source: <http://www.businessweek.com/ap/financialnews/D9KRGURG0.htm>

34. *January 19, Kaiser Health News* – (National) **Hospitals try to curb emergency room crowding.** Ochsner Medical Center is one of a growing number of emergency departments trying new approaches to ease crowding. The efforts have added urgency as some experts predict the problem could worsen in coming years. They worry that as millions of people suddenly gain health coverage in 2014 under the new federal health law, they may have trouble finding primary care doctors and will turn to hospital emergency departments instead. The hospital efforts to address the problem have ranged from high-tech options such as smart phone programs that let patients compare waiting times at local hospitals to something as mundane as staggering nursing shifts to better match patient traffic. “Fast tracks,” or clinics for patients with simple complaints, are also common. Some hospitals are looking at shaking up and re-engineering their procedures. Ochsner, for instance, created an emergency department protocol called “qTrack.” The sickest patients go back immediately to the emergency department’s traditional beds, but others go quickly into separate treatment areas with a nice comfortable recliner or to a procedure room for stitches or a cast. Even as emergency departments work on new initiatives, some experts argue that attention should be focused instead on the hospital as a whole. A Rand Corp. scholar and an emergency care physician said such “workarounds” let hospitals off the hook. “The reality is the rest of the hospital doesn’t want to deal with the fact that the overcrowded ER is a sure absolute sign of a poorly managed hospital.”

Source: http://www.msnbc.msn.com/id/41136840/ns/health-health_care/

35. *January 18, Homeland Security Today* – (National) **Data monitoring can aid in hospital infection prevention.** As the use of electronic surveillance systems (ESSs) in hospitals for infection prevention and control programs has become more widespread, a new study found that despite evidence these systems may improve efficiency of data

collection and potentially improve patient outcomes, ESSs actually remain relatively uncommon in infection prevention and control programs. The paper, “Electronic Surveillance Systems in Infection Prevention: Organizational Support, Program Characteristics, and User Satisfaction,” by researchers at the Texas Health Science Center, published in the American Journal of Infection Control, found “only 23 percent (44/192) of responding infection prevention and control departments had an ESS.” No statistically significant difference was seen in how and where infection preventionists who used an ESS and those who did not spend their time. But as the paper pointed out, “little is known about the characteristics of hospitals that have a ESS, user satisfaction with ESSs, and organizational support for implementation of ESSs.”

Source: <http://www.hstoday.us/briefings/daily-news-briefings/single-article/data-monitoring-can-aid-in-hospital-infection-prevention/c875f22d11816b36c3729c1f4d6137bb.html>

[\[Return to top\]](#)

Government Facilities Sector

36. *January 20, Associated Press* – (National) **9 LA schools reopen with extra security after police officer’s shooting; suspect sought.** Nine schools in the Woodland Hills area of the west San Fernando Valley in Los Angeles, California, that were locked down for hours after a school police officer was shot near a campus January 19, reopened January 20 under heavy security, a district official said. School district police and city officers patrolled at El Camino Real High School and other campuses in the area. Crisis counselors also were on hand, but normal classes were held. “We feel that our students are safe and secure,” but the extra security presence may comfort anxious pupils, a spokesman for the Los Angeles Unified School District said. The shooting happened January 19 on a street just outside El Camino Real. Some 9,000 students were held in classrooms for hours at area middle, elementary, and high schools as police searched for the suspect. Some were finally allowed to leave long after dark. A school police officer was struck in the chest by a bullet when he confronted a man breaking into cars, but his body armor stopped the round, authorities said. More than 350 police officers, sheriff’s deputies and California Highway Patrol officers scoured 7 square miles around the school. Three schools in the “hot zone” — the immediate area near the shooting — kept students in classrooms for hours without access to food or bathrooms, the spokesman said.

Source: <http://www.latimes.com/news/nationworld/nation/wire/sns-ap-us-la-school-officer-shot,0,2787380.story>

37. *January 19, Associated Press* – (International) **US suspends Peace Corps program in Niger, evacuates volunteers over security concerns.** The Peace Corps has suspended its operations in Niger and evacuated its workers from the west African nation due to security concerns following the kidnapping and murder of two French citizens claimed by an al-Qaida affiliate. The Peace Corps said January 18 that all 98 of its Niger-based volunteers are safe and are now in another country. The move marks the first time the agency has halted its programs in Niger since it started working there in 1962. It said it

would review safety and security in the country before restarting its work there. The suspension came after a purported spokesman for al-Qaida's North Africa branch, al-Qaida in the Islamic Maghreb, claimed responsibility the week of January 10 for kidnapping the two Frenchmen who later died during a failed rescue attempt.

Source:

http://www.google.com/hostednews/canadianpress/article/ALeqM5g_9uGdzXHWiwaDjCA_xhV-KnUiEA?docId=5692655

38. *January 19, Associated Press* – (Utah) **Utah State reopens ROTC building after threat.** The ROTC building at Utah State University in Logan, Utah reopened January 19 after being closed for 2 days following a message threatening armed violence. A university spokesman said a behavioral intervention team of police officers and counselors met with a student accused of making the threat. The spokesman would not specify the threat, but said it was enough to prompt university action. No charges will be filed. The incident came on the first day of Utah State's spring semester.

Source: <http://www.abc4.com/content/news/state/story/Utah-State-reopens-ROTC-building-after-threat/qINiWgQ92EK67DeEEF-xNw.csp>

For another story, see item [49](#)

[\[Return to top\]](#)

Emergency Services Sector

39. *January 20, Homeland Security Today* – (International) **More VBIEDs detonated south of the border.** As the largely narco-fueled violence in Mexico escalates, the country's crime cartels have resorted to using one of jihadist terrorists' most lethal weapons — the car bomb. Mexico's Secretariat of Public Security (SSP) announced that a "vehicle-borne improvised explosive device" (VBIED) exploded January 19 in front of a muni-police station in Linares, Nuevo Leon, Mexico. The car was a white Jetta from Nuevo Leon and had been parked in the reserved parking space of a high ranking police department official. The SSP further confirmed a second car bomb was detonated in front of a police station in San Nicolas hours later. The VBIED detonated in San Nicolas was in a car that reportedly was abandoned by a man dressed in black just minutes before it exploded. According to eyewitness accounts, three women had jumped out of the vehicle that blew up in Linares only minutes after they allegedly left the scene. Although there were no reported injuries, there was extensive property damage, including to two nearby vehicles that belonged to a local police official.

Source: <http://www.hstoday.us/briefings/daily-news-briefings/single-article/more-vbieds-detonated-south-of-the-border/c9dc67a90ce542fbd748ac9126b4a89c.html>

40. *January 19, Reuters* – (New Mexico) **Former N.M. sheriff charged with selling police gear.** The former sheriff of Santa Fe County, New Mexico, was arrested and taken to the jail he used to run January 19, accused of embezzling county property, including protective vests and other police gear which he allegedly sold on the Internet. The two-term sheriff resigned in November after admitting he auctioned off county

property on Ebay. The district attorney said he surrendered peacefully at his attorney's office in Santa Fe and was booked into the county jail. Bond was set at \$25,000. He faces 252 charges of embezzling and selling \$60,000 in public property that also included gun holsters, handcuffs, digital recorders, ink cartridges, flashlights, and police duty belts from January of 2007 to November 2010. If convicted on all counts he could be sentenced to a maximum of 250 years in prison. A state police captain said authorities were tipped off in September 2010 by a lawman in Texas who said he had purchased a bullet-proof vest from the sheriff over the Internet. The former sheriff said his family had been facing financial problems. The district attorney said he had been using the proceeds from the sales for gambling and other "personal habits."

Source: <http://www.reuters.com/article/idUSTRE70J0R420110120>

For more stories, see items [21](#) and [34](#)

[\[Return to top\]](#)

Information Technology Sector

41. *January 20, IDG News Service* – (International) **Soundminer Trojan horse steals Android phone data.** Researchers have developed a low-profile Trojan horse program for Google's Android mobile OS that steals data in a way that is unlikely to be detected by either a user or antivirus software. The malware, called Soundminer, monitors phone calls and records when a person, for example, says their credit card number or enters one on the phone's keypad, according to the study. Using various analysis techniques, Soundminer trims the extraneous recorded information down to the most essential, such as the credit card number itself, and sends just that small bit of information back to the attacker over the network, the researchers said. The study was done by researchers from the City University of Hong Kong and Indiana University.

Source:

http://www.computerworld.com/s/article/9205627/Soundminer_Trojan_horse_steals_Android_phone_data

42. *January 19, Computerworld* – (International) **Researcher releases attack code for just-patched Windows bug.** Attack code for a Windows vulnerability that Microsoft patched the week of January 9 was released by a researcher one day after the company fixed the flaw. The bug, which Microsoft rated "critical" — its highest threat ranking — was first reported more than 9 months earlier when its discoverer used it in a one-two punch against Internet Explorer 8 (IE8) that won him \$10,000 in a hacking challenge. The researcher used the vulnerability to sidestep one of Windows 7's most important anti-exploit defenses, ASLR (address space layout randomization). "I used this to get rid of ASLR, and another vulnerability to bypass DEP," he said. DEP, or data execution prevention, is another protection technology Microsoft relies on to make it difficult for attackers to execute their malicious code on Windows. He posted one version of the exploit he used at Pwn2Own on his own Web site January 12. That was the day after Microsoft patched the vulnerability in Microsoft Data Access Components (MDAC), a set of components that lets Windows access databases such as Microsoft's

own SQL Server. The flaw is in the MDAC ActiveX control that allows users to access databases from within IE.

Source:

http://www.computerworld.com/s/article/9205522/Researcher_releases_attack_code_for_just_patched_Windows_bug

43. *January 19, Computerworld* – (International) **Oracle patching fewer database flaws as it adds more products.** Oracle Corp.'s ability to address vulnerabilities in its core database technologies may be hampered by the vast number of products the company now must manage, security experts say. For example, the list of Oracle's quarterly security updates released January 18 includes only six patches for security flaws in the company's flagship database products. The other 60 patches released fix bugs in Oracle's Fusion middleware technologies, its supply chain and CRM software, and products gained from its acquisition of Sun Microsystems early in 2010. The small number of database patches does not necessarily mean Oracle technology is becoming more secure, the director of security at Application Security Inc.'s Team Shatter vulnerability assessment group said. Rather, it likely shows the company does not have the capacity to fix the full list of Oracle database flaws reported to it in a timely fashion, said the director, whose team of researchers discovered three of the six database flaws addressed in an update released the week of January 16. "The number of database fixes from Oracle has really gone down," he said. "But that's not because of a lack of vulnerabilities. They have apparently reassigned their priorities and are choosing not to fix all the database vulnerabilities that are reported to them. It appears that they are losing some of the DBMS focus and are getting spread too thin on other stuff."

Source:

http://www.computerworld.com/s/article/9205560/Oracle_patching_fewer_database_flaws_as_it_adds_more_products

44. *January 19, IDG News Service* – (International) **Obama, Ballmer urge China to step up IP enforcement.** The U.S. President and the CEO of Microsoft pressed the President of China January 19 to step up enforcement of intellectual property rights in his country. In a move that indicates China's decade of efforts to crack down on software piracy has failed in the eyes of foreign businesses, Microsoft's CEO met with the U.S. President and the Chinese leader at the White House in Washington, D.C. to push the issue. "So we were just in a meeting with business leaders, and [the CEO] of Microsoft pointed out that their estimate is that only 1 customer in every 10 of their products is actually paying for it in China," the U.S. President told a press conference. The U.S. President said the Chinese President had agreed to take action. Under pressure from foreign business leaders over the past 10 years, China periodically arrests the manufacturers and sellers of counterfeit DVDs and CDs. Some discs, often sold on street corners or in public markets, are Microsoft operating systems sold at fractions of the market price.

Source:

http://www.computerworld.com/s/article/9205599/Obama_Ballmer_urge_China_to_step_up_IP_enforcement

For another story, see item [12](#)

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

45. *January 19, San Bernardino Press-Enterprise* – (California) **AT&T and Verizon work on rain damage.** At least 500 residents in Riverside County, California, are still without telephone, Internet, or television service a month after persistent rainstorms ravaged the inland region. AT&T and Verizon are still in the thick of repairing underground cable and telephone lines damaged by flooding during December’s severe storms. As of 2 weeks ago, about 4,500 customers still had problems with AT&T service in Riverside County after the precipitation. Statewide, the telecommunications company reported having 70,000 “trouble tickets” pending at that time from customers reporting outages and issues related to the rain. Verizon, which serves San Bernardino County, would not say how many of its customers were affected by flooding to its underground cables. As of January 19, the number of affected AT&T customers within Riverside County who were still reporting problems with their wired phone service, Internet, and television had dropped to 500. Statewide, the number had dropped to 21,000.

Source:

http://www.pe.com/localnews/stories/PE_News_Local_D_cable20.12494aa.html

46. *January 19, NetworkWorld* – (International) **At Black Hat, fake GSM base station trick targets iPhones.** While his Black Hat DC Conference demonstration was not flawless, a University of Luxembourg student January 19 showed it is possible to trick iPhone users into joining a fake GSM network. The student showed how to cobble together a laptop using open-source software OpenBTS and other low-cost gear to create a fake GSM transmitter base station to locate iPhones in order to send their owners a message. A number of iPhone users in the room expressed surprise they had gotten a message asking them to join the network. The student, who is researching vulnerabilities in cellular networks, said that with the right equipment, the range for the rogue GSM station he built can be 35 kilometers. The student’s attack would allow him to take advantage of iPhones lured into his rogue base station to “enable and disable auto-answer on the iPhone” he said, or with an attack payload to record the audio on the iPhone, store it in RAM and then transmit the data that was sniffed. The student said he does not want to encourage data theft, but he does want to get carriers and vendors to improve security in the wireless networks. He noted technology such as femtocells could be used to replace the OpenBTS software, which would only amplify

the types of attacks he is investigating.

Source:

[http://www.computerworld.com/s/article/9205559/At Black Hat fake GSM base station trick targets iPhones](http://www.computerworld.com/s/article/9205559/At_Black_Hat_fake_GSM_base_station_trick_targets_iPhones)

[\[Return to top\]](#)

Commercial Facilities Sector

47. *January 20, Lower Hudson Journal News* – (New York) **2 Yonkers apartment buildings evacuated as adjacent unoccupied building burns.** About 45 people were removed from two apartment buildings as about 90 Yonkers, New York firefighters battled a suspicious four-alarm fire January 20 in an adjoining unoccupied building, the fire commissioner said. Firefighters were called to 94 St. Andrews Place at 2:15 a.m. They were met by heavy volume of fire coming from the two top floors, he said. As they battled the fire, the roof collapsed in the front of the structure. The roof was in danger of collapsing in the rear of the burning building also, firefighters said. None of the residents from adjacent two, 5-story apartment buildings at 90 and 100 St. Andrews Place were reported injured. “They were evacuated because of the danger of the fire spreading,” the fire commissioner said. All three 5-story buildings are connected by common parapets. Firefighters were able to stop the fire from endangering the two occupied buildings. “It is a very suspicious fire,” the fire commissioner said. He said someone had tried to ignite the building several times in recent months.
Source: <http://www.lohud.com/article/20110120/NEWS02/110120002/-1/newsfront/2-Yonkers-apartment-buildings-evacuated-as-adjacent-unoccupied-building-burns->
48. *January 20, Maple Shade Progress* – (New Jersey) **Chemical explosion in Maple Shade sends one to the hospital.** Maple Shade, New Jersey, firefighters responded to an explosion January 18 that blew out the windows of a unit at the Southern Arms apartment complex, sending one man to the hospital for treatment of burns. According to the Maple Shade Fire Department chief, the blast and subsequent fire was brought on by a reaction between household chemicals that were being stored under the kitchen sink. “We are still trying to put the pieces of the puzzle together. Some of the things just do not add up. We are looking into everything.” He said the fire was definitely accidental and there was no malicious intent. The kitchen and the living room of the unit sustained damage and some windows of the unit were blown out by the explosion. Residents of the building were evacuated at approximately 8 p.m. and were able to return less than 2 hours later, he said. No other units of were damaged. A resident of the damaged apartment suffered minor chemical burns to his legs and was taken to a local hospital for treatment.
Source: http://www.southjerseylocalnews.com/articles/2011/01/20/maple_shade_progress/news/doc4d383ad65e829634598515.txt
49. *January 19, ArkansasNews.com* – (Arkansas) **Man indicted in connection with bomb at polling place.** A federal grand jury has indicted an Arkansas man suspected of trying

to bomb a Carroll County polling place in June. The indictment filed in U.S. District Court in Harrison, Arkansas, charges the 40-year-old man with possession of an unregistered destructive device, the U.S. attorney for Arkansas' Western District, said January 19. He is scheduled to be arraigned in U.S. District Court in Fort Smith January 26. If convicted, he could be sentenced to up to 10 years in prison and fined up to \$10,000. Authorities said they found an improvised explosive device inside a 12-ounce soda pop can outside Osage Baptist Church in Osage June 8, 2010. At the time, the church was being used as a polling place for the primary runoff election. Bentonville's bomb squad destroyed the device with no injuries. Authorities said bomb-making materials later were found in a Huntsville residence the suspect had owned.

Source: <http://arkansasnews.com/2011/01/19/man-indicted-in-connection-with-bomb-found-at-polling-place/>

50. *January 19, KGO 7 San Francisco* – (California) **Woman jailed after pipe bombs found in storage.** Police are still trying to figure out why a 40-year-old Concord, California woman had five pipe bombs in a rented storage locker in Pacheco, California. She is being held in the Contra Costa County jail in Martinez, on \$500,000 bail. She is charged with possession of an explosive device for the four bombs found inside a backpack inside a locker she rented at Affordable Storage on North 1st Avenue. A fifth bomb was found outside the backpack. "They varied in sizes from 4 or 5 inches to 8 inches. Inside one of the pipe bombs, we are checking to see if they were in more, we found glass shards. Specifically, when it explodes it was meant to hurt someone when those shards come out of the pipe bomb," a commander with the Contra Costa Narcotic Enforcement Team said. Two others arrested at the storage facility have been released and are not believed to be connected to the explosives. A small amount of methamphetamine was also located at the storage unit. The commander said his agents are trying to determine the purpose of the explosives, and that the suspect is not cooperating with investigators.
- Source: http://abclocal.go.com/kgo/story?section=news/local/east_bay&id=7907676

For more stories, see items [32](#) and [55](#)

[\[Return to top\]](#)

National Monuments and Icons Sector

51. *January 20, Salem News* – (Ohio) **Fire at historic home.** Firefighters responded to a fire at the historic John Street House in Salem, Ohio, at 4:50 p.m. January 19. The house was built in 1838 by the son of Salem's founder, and the house was added to the National Register of Historic Places in 1973. It was famous for its role as an Underground Railroad Station during years preceding and during the Civil War. A famed abolitionist was a frequent guest at the house. A marker was placed in front by the Daughters of Union Veterans of the Civil War in 1941. The cause of the fire was electrical, a fire captain said.

Source: <http://www.salemnews.net/page/content.detail/id/536484/Fire-at-historic-home.html?nav=5007>

52. *January 19, KITV 4 Honolulu* – (Hawaii) **Snow, ice close Haleakala park.** Snowfall and icy road conditions in Hawaii prompted officials at Haleakala National Park to close January 19. Snow fell overnight and could be seen from all around Maui. Park officials closed the park at the 7,000-foot level early in the morning because of the conditions. They began turning visitors away at the gate when the parking lot filled up and rain started falling. The temperatures did not begin rising in the morning and the rains caused the icy road conditions, park officials said. The park may reopen in the afternoon, they said.

Source: <http://www.kitv.com/news/26543168/detail.html>

[\[Return to top\]](#)

Dams Sector

53. *January 20, Eugene Register-Guard* – (Oregon) **Workers unlog debris from gate at Leaburg Dam.** The Eugene Water & Electric Board (EWEB) in Oregon — with the help of a Wildish Construction excavator — January 19 cleared a massive clump of logs, root wads and other woody debris that had blocked a gate at Leaburg Dam since the night of January 16. The debris swept down the river during a storm that dumped 5 inches of rain in some areas. Coupled with warm temperatures that brought rapid snowmelt, the rain sent water surging at 35,000 cubic feet per second (cfs) down the river January 17. A more normal flow for this time of year, according to U.S. Geological Survey water gauges, is 4,000 to 5,000 cfs. The debris jammed one of three roll gates on the dam, which controls the flow of water on the McKenzie River. Crews worked from 4 p.m. until midnight January 18 to try to free the wood stuck in the 100-foot-wide roll gate, then came back first thing January 19 to get after it again. They were able to punch through the debris and get it moving by about noon, according to an EWEB news release. The gate appears to be working normally, but the utility is examining it for damage, a spokesman said. Some of the logs the river flung down measured more than 100 feet in length.

Source: <http://www.registerguard.com/csp/cms/sites/web/news/cityregion/25794025-41/dam-debris-eweb-leaburg-gate.csp>

54. *January 20, Fayetteville Observer* – (North Carolina) **Hope Mills board told hole under dam should be closed in week.** The Fayetteville, North Carolina mayor told the board January 19 that work is under way on temporarily closing the hole under the failed Hope Mills Lake dam and should be completed within a week. Earlier in January, workers were underneath the structure taking pictures and video and collecting samples in an effort to determine why the dam was breached in June. The hole would have to be reopened once work begins on repairing the dam, a process the mayor said could take years. The town has been without the lake since June 17, when vinyl sheeting in the foundation of the dam gave way. Earlier this month, the board voted to

pay \$100,000 to MBP Engineering of Raleigh, the firm overseeing the investigation.
Source: <http://www.fayobserver.com/articles/2011/01/20/1064625?sac=Local>

55. *January 20, Nashville Tennessean* – (Tennessee) **Gaylord repairs levee at Opryland Hotel but doesn't raise it.** Some \$1 million to \$2 million in flood repairs are under way on the levee at the Opryland Hotel in Nashville, Tennessee. But that work does not include raising the height of the earthen berms and concrete barriers that failed to keep the Cumberland River from spilling into the resort as the May flood reached its peak last year. Raising the levee is a separate \$10 million project that the Gaylord Entertainment CEO has said he is ready to launch on his own unless he sees progress on a community-wide flood prevention plan. Gaylord board members have discussed raising the levee, but no decision has been made on whether to act independently or wait on a broader plan.

Source:

<http://www.tennessean.com/article/20110120/BUSINESS01/101200342/2221/BUSINESS>

56. *January 19, KAPS 660AM Washington* – (Washington) **Repairs made on damaged dike.** Skagit County's Dike District 17 in Mount Vernon, Washington, was finally able to get permission from the U.S. Army Corps of Engineers the night of January 17 to conduct emergency repairs on a damaged dike. The section of dike is located behind the Riverbend RV Park across Riverbend Road from the Mount Vernon Walmart, but they report no breach of the levee. Tons of riprap rock were dumped into a weak area about 80 feet long the night of January 17 and early the next morning.

Source: <http://www.kapsradio.com/kaps-radio-660am-news-headlines/repairs-made-on-damaged-dike/>

57. *January 19, Kent Reporter* – (Washington) **Green River's Hanson Dam performs well during heavy rain.** The Howard Hanson Dam in Washington performed well during recent heavy rains to help control flooding along the Green River, the U.S. Army Corps of Engineers said. The Corps held water behind the dam that pushed the reservoir level to a peak of 1,155 feet above sea level. That is above an elevation (1,147 feet) that triggers increased on-site monitoring. The Corps has held Hanson Dam outflows to around 7,000 cubic feet per second (cfs), while inflows peaked above 20,000 cfs. The Corps is operating the dam to keep flows along the Green River at Auburn at 10,500 cfs, below the 12,000 cfs level of concern for levees from Auburn downstream to Kent, Tukwila, and Renton. Levee patrol teams remained out January 19 in the Green River basin monitoring conditions and communicating back to the Seattle District reservoir control center and emergency operations center. Flows above or near 9,000 cfs along the Green River trigger 24 hour per day monitoring. There is a risk of flooding for property owners along the non-leveed middle Green basin, the part of the river upstream from Auburn to Hanson Dam. The flows do not present flooding concerns for highly populated areas downstream, including Auburn, Kent, Tukwila, or Renton. The Corps works to keep the reservoir empty at Hanson Dam along the Green River until storage is required for flood risk management. The dam had an empty

reservoir January 14.

Source: http://www.pnwlocalnews.com/south_king/ken/news/114241144.html

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact Information

Content and Suggestions:

Send mail to 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

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.