Homeland Security

Daily Open Source Infrastructure Report for 18 November 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- NextGov reports that information security weaknesses continue to plague Los Alamos National Laboratory. According to the Government Accountability Office (GAO), the lab failed to allow only authorized users access to the network. The GAO identified numerous network vulnerabilities in several critical areas of the laboratory, which manages operations at nuclear facilities. (See item **9**)
- Reuters reports the U.S. Securities and Exchange Commission (SEC) charged two companies, Mantria, Speed of Wealth, and four individuals with running a $30 million Ponzi scheme that targeted elderly investors and people nearing retirement who were seeking environmentally friendly investments. (See item **14**)

Fast Jump Menu

Energy Sector

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

1. *November 17, Lower Hudson Journal News* – (New York) **Con Ed fire spurs oil cleanup along Bronx River.** An explosion at a Consolidated Edison substation has set

off a massive oil-spill cleanup along the Bronx River. Scores of workers are cleaning up an unknown quantity of a light, clear oil similar to mineral oil that flowed into the city's storm sewer system on November 4 when a 345-kilovolt transformer containing 30,000 gallons of the fluid caught fire. A machine malfunction created an electrical arc that ignited the oil at 152 Kingston Ave. in the Dunwoodie neighborhood. The resulting smoky fire was controlled in 20 minutes, and no one lost power from the event. Much of the oil, which was used as a dielectric fluid to cool the transformers, burned or remained on-site, but some of it mixed with the water used to quell the flames and escaped into the city's sewer system, where it flowed into the Bronx River near the Cross County Parkway. A Con Edison spokesman said that cleanup of the escaped oil began the day of the fire. According to the state Department of Environmental Conservation (DEC), the fluid initially eluded capture by booms, a type of sponge that absorbs oil, because of fast-moving water along the river. Crews hired by Con Edison are now working in areas where the river's flow is slower, mainly near the Bronx Zoo and the New York Botanical Garden. The sewer pipe that delivered the oil to the river is also being cleaned. Much of the oil has mixed with fallen leaves, and crews are using large vacuum trucks to extract the oil and leaves from the riverbanks. The DEC has not discovered any wildlife injured by the oil spill, but the agency's biologists are checking the contaminated area.
Source: http://www.lohud.com/article/20091117/NEWS02/911170335/-1/newsfront/Con-Ed-fire-spurs-oil-cleanup-along-Bronx-River

2. *November 17, San Francisco Examiner* – (California) **Overflowing tank pegged as culprit.** An overfilled fuel tank caused a ship to spill hundreds of gallons of oil into San Francisco Bay last month after operators failed to use the required containment equipment. Original reports blamed a ruptured fuel line. West Coast shipping services company Foss Maritime was filling the Dubai Star tanker's fuel tanks near San Francisco's southern shoreline October 30 when 400 to 800 gallons overflowed. Foss Maritime's barge was equipped with legally mandated oil containment equipment, but operators failed to use it to control the spill, according to a California Office of Spill Prevention and Response counselor. At least 36 birds were killed by the toxic bunker fuel, which washed onto East Bay shorelines. Cleanup efforts were still under way November 16 at Robert Crown Memorial Beach in Alameda. The onboard oil containment equipment, known as the boom, was not deployed after the spill because the barge and all ship workers were on the other side of the vessel, he said. Two tanks were being successively filled using the same fuel line, but fuel continued to be pumped into the first tank after it became full, causing it to overflow and spill, according to the counselor. He said he expects to meet with investigators from his department on November 19 to discuss their findings. "We're looking at the vessel transfer plan," he said. "I've not seen that document, so I don't know if there's supposed to be somebody on both sides of the vessel." A fuel-line valve that should have prevented the overflow is being inspected, according to the counselor. "It's either a situation where the valve wasn't fully closed or it was defective," he said. California regulations require fuel barges to carry oil-absorbing, buoyant boom or to preboom around a ship before fueling begins.

http://www.sfexaminer.com/local/Overflowing-tank-pegged-as-culprit-70257372.html

3. *November 16, Columbus Local News* – (Ohio) **South side power outage caused by copper wire theft.** A power outage in the Grove City, Ohio area on November 16 was caused by thieves, authorities have said. The outage affected more than 11,000 people overall, about 2,000 of whom were inside the boundaries of Grove City. A Grove City police captain said police first received notice of the outage about 8:30 a.m., and power was restored by about 11:30 a.m. The captain said Grove City police heard conflicting stories about the cause of the blackout, but the outage was caused by thieves stealing copper wire from a substation on McComb Road, in an area north of the boundaries of Grove City. American Electric Power (AEP) released a statement late in the afternoon November 16 that confirmed the outage was due to a theft. There was no outage until AEP officials became aware of the theft shortly after 8 a.m. on November 16. They had to shut down power in order to make repairs.
Source: http://www.columbuslocalnews.com/articles/2009/11/16/multiple_papers/news/allgcblack_20091116_0525pm_1.txt

[Return to top]

Chemical Industry Sector

4. *November 16, Fort Myers New-Press* – (Florida) **All lanes of San Carlos Blvd. open following chemical spill.** According to the Lee County Sheriff's Office, a pool truck containing chlorine was struck by another vehicle. It was reported that a total of 15 gallons of chlorine spilled. Several containers of muriatic acid also fell off the truck but did not spill. Two people were transported to the hospital, but the extent of their injuries is unknown. All lanes on the Matanzas bridge are now open.
Source: http://www.news-press.com/article/20091116/NEWS0117/91116025/1075/Chemical-spill--crash-close-both-directions-of-San-Carlos-Blvd.

5. *November 16, Associated Press* – (Oregon) **Tractor crashes at Umatilla Chemical Depot.** Police are looking for a suspect who fled after crashing a large tractor through a fence at the Umatilla Chemical Depot. A depot spokesman says the tractor did not get near the chemical weapons storage area, but security remains high following Sunday night's incident. The spokesman says the Federal Bureau of Investigation responded, but depot security and the Umatilla County sheriff are handling the investigation.
Source: http://www.ktvz.com/Global/story.asp?S=11516146

6. *November 16, KSTP 5 St Paul* – (Minnesota) **Ammonia accident in Rosemount kills one.** An ammonia accident at a trucking company facility in Rosemount killed one person and critically injured another. A Rosemount police officer said the accident happened around 6 p.m. at CF Industries. Police do not know what led to the accident, but the officer said they believe ammonia was being loaded into a truck at the time. The

person who was critically injured was airlifted to Regions Hospital in St. Paul. Two officers also went to Regions for evaluation, but they were able to drive themselves. Emergency crews were still on scene as of 8 p.m. Monday. He said the Occupational Safety and Health Administration will investigate.
Source: http://kstp.com/news/stories/S1257054.shtml?cat=1

[Return to top]

Nuclear Reactors, Materials and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

7. *November 15, Alibaba* – (International) **BYD dives after Nokia recall.** Nokia is recalling millions of cellphone chargers manufactured this year by the battery-making arm of BYD Co. Nokia, the largest mobile phone maker globally, announced on November 16 that it will offer a free replacement for three kinds of defective chargers, citing a risk of electrocution due to a loose plastic cover on some of the models. It is a precautionary measure, both companies said, since no injury has been reported. While Nokia did not name the number of customers affected, reports have estimated the recall applies to 14 million chargers. The specific phone charger models affected by the recall are the AC-3E and AC-3U made between June 15 and August 9, 2009, as well as the AC-4U model made between April 13 and October 25, 2009 according to a BYD statement. Nokia's last recall was in 2007, when it found 40 million lithium-ion batteries produced by Japanese manufacturer Matsushita Battery Industrial posed a risk of overheating. BYD, which also makes chargers for Motorola, will cover the costs of the recall.
Source: http://news.alibaba.com/article/detail/cars/100200848-1-byd-dives-after-nokia-recall.html

[Return to top]

Defense Industrial Base Sector

8. *November 17, Shephard Group Limited* – (International) **BAE Systems Advanced Precision Targeting System begins final testing.** BAE Systems has entered the final phase of testing on its Advanced Precision Kill Weapon System (APKWS), a technology that increases the accuracy and cost-effectiveness of airborne weapon systems. The tests seek to confirm the production readiness of the APKWS rocket and its ability to meet Navy and Marine Corps requirements, including safely launching from a helicopter, and reliably acquiring, tracking, and hitting laser-designated targets. In the most recent testing, a laser-guided rocket fired from a U.S. Marine Corps Cobra helicopter hit a stationary target. This test firing initiated a sequence of more than 20

firings that will comprise the program's final test phase, to be completed by the end of 2009. With completion of this contractor test flight, BAE Systems and the Navy are preparing for Navy demonstration test flights and full government qualification testing. APKWS will enter production in 2010. APKWS has hit its targets 18 times since September 2002, including five shots from helicopters involving several air crews and various mission scenarios. The low-cost, low-yield precision munition system turns a standard 2.75-inch unguided rocket to a smart, highly precise laser-guided missile. Because it uses standard launchers, the system requires no platform integration or aircraft modifications, and the mid-body design of its guidance section enables use of existing warheads, fuses, and rocket motors. APKWS can be fired from any helicopter that can launch 2.75-inch rockets, including the AH-1 Cobra, UH-1 Huey, OH-58 Kiowa Warrior, and AH-64 Apache. The Navy assumed acquisition executive oversight of the program in 2008 and has fully funded it for production. BAE Systems has been the APKWS prime contractor since 2006.
Source: http://www.shephard.co.uk/news/4531/bae-systems-advanced-precision-targeting-system-begins-final-testing/

9. *November 16, Nextgov* – (New Mexico) **Los Alamos National Lab again under fire for weak computer security.** Information security weaknesses continue to plague Los Alamos National Laboratory, according to the Government Accountability Office (GAO), which reported on Friday that the lab failed to allow only authorized users access to the network. In its report last week, GAO identified numerous network vulnerabilities in several critical areas of the laboratory, which manages operations at nuclear facilities. Among the weaknesses were failures to identify and authenticate users, authorize user access, encrypt classified information, monitor compliance with security policies, or check that security settings are up to date. The National Nuclear Security Administration (NSAA) oversees the laboratory, which is managed by Los Alamos National Security, a consortium of contractors. According to GAO, NNSA policy states that individuals must not share passwords except in emergency circumstances or when there is an overriding operational necessity, and passwords on sensitive systems should be changed at least every six months. The administration also requires the lab use two-factor authentication whenever possible. Two-factor authentication requires a user to provide two sets of identity such a username and password, and possibly a smart card or a fingerprint. "[The lab] did not always manage passwords securely on the classified computer network," GAO investigators said. "As a result of this weakness, increased risk exists that insiders with malicious intent could guess the passwords of other individuals and use them to gain inappropriate access to classified information." In addition, users were granted access to more computer files than needed to perform their duties and classified systems were not configured with necessary security controls, according to the report. Although the lab made some improvements to information security in the past couple of years, the latest report highlights "a number of high-profile security lapses," GAO noted.
Source: http://www.nextgov.com/nextgov/ng_20091116_2938.php?oref=topnews

10. *November 15, Fort Worth Star-Telegram* – (National) **F-35 is far behind schedule and over budget, reports show.** Work on the F-35 joint strike fighter program is far behind

schedule and over budget despite the completion Saturday of a milestone test flight. Reports prepared by the Defense Contract Management Agency for Defense Department officials show that Lockheed and other contractors are months late on deliveries of test airplanes and components for future production aircraft. The program is even farther behind on testing, and the reports say Lockheed could exhaust its development budget within a year. Problems cited in the documents support a recent Pentagon assessment that F-35 development will require two more years and billions of additional dollars. The Pentagon's top weapons buyer has called a meeting for this weekend to address the reports' conclusions and prepare recommendations for the Secretary of Defense. The senior Lockheed executive running the F-35 program said in an interview that the reports are largely accurate. But the worst of the delays have been surmounted and good progress is now being made, he said. The flight Saturday was only the fourth by a test airplane since the contract to develop the next-generation combat aircraft was awarded to Lockheed in late 2001. The monthly reports prepared for Pentagon F-35 program managers show that Lockheed and its subcontractors badly trail the most recent revised schedule, adopted in May 2008. Key points include: Production of test aircraft is running about six months behind; Lockheed has had significant difficulty assembling the wing and major components; suppliers are late delivering finished parts and components not only because of manufacturing problems but also because of repeated design and engineering changes; and Lockheed is exceeding cost targets and at current spending rates would exhaust its budget in fiscal 2011, which begins October 1.
Source: http://www.star-telegram.com/local/story/1764028.html

[Return to top]

Banking and Finance Sector

11. *November 17, CNBC* – (National) **Financial fraud task force to be announced.** The Treasury Department, Justice Department, Department of Housing and Urban Development (HUD) and the Securities and Exchange Commission (SEC) plan to form a taskforce to devote more resources to discovering and punishing those who commit financial fraud, NBC News has learned. The task force will focus particularly on fraud in the housing and securities industries, officials said on November 16. A government announcement about the program is expected around noon, New York time. The Attorney General, Treasury Secretary, HUD Secretary and the director of enforcement at the SEC will speak from the Justice Department. No enforcement actions will be announced, but the purpose of the task force will be explained, officials said.
Source: http://www.cnbc.com/id/33985024

12. *November 16, IDG News Services* – (International) **MasterCard to authenticate online transactions by phone.** In the face of mounting threats from hackers, MasterCard said on November 16 it will use mobile phones to improve security for online transactions. The added layer of security comes from a one-time password that the user is asked to enter when approving a transaction. The password is either sent via an SMS (Short Message Service) or created by an application that runs on a

smartphone or a phone that supports Java. The goal is to improve users' protection against phishing and man-in-the-middle attacks, which are growing problems in the e-banking and e-commerce world, according to MasterCard. There is no fool-proof way to protect against these attacks, but the fact that the new passwords can be used only once limits the potential damage they could inflict, according to a senior business leader and head of chip product management at MasterCard. The first services to use the improved security will become available during the first half of next year, the business leader said. MasterCard is not building these systems itself, but will work with a number of partners. It has so far signed deals with three vendors, but is not ready to name them, according to the business leader. The use of mobile phones for payments and other related services is slowly gaining ground all over the world. MasterCard on November 16 also announced the Mobile Payments Gateway. It will, for example, let users pay, send and receive money and keep track of activities via alerts on the their mobile phone, MasterCard said.
Source:
http://www.computerworld.com/s/article/9140946/MasterCard_to_authenticate_online_transactions_by_phone

13. *November 16, CNET News* – (National) **Senate to disclose findings in Web 'mystery charge' probe.** So-called mystery charges that have appeared on some of their customers' credit card statements will come under scrutiny at a hearing held by the U.S. Senate Committee on Commerce, Science and Transportation. At the center of the federal probe are Webloyalty, Affinion, and Vertrue, companies that make "cash-back" and coupon offers to consumers and charge them monthly fees to enroll in their loyalty programs. The reason the government is involved is that for years, scores of online shoppers have asserted they were signed up for the programs without their consent. An example of this deceptive practice: An ad pops up just as the customer completes a transaction at an online retail site. It is packed with fine print and it's not easy to see how to get past the page to complete the purchase. What is clear is that all it takes to move off the page is to enter an e-mail address. A shopper may think that entering an e-mail cannot hurt them and is not aware a marketer has their credit card information. But what those who enter their address are often unaware of is that they are authorizing the retail store to allow Web Loyalty, Affinion, Vertrue, or other similar marketers to charge their credit cards. There are cases where shopper does not discover the monthly charges on their credit card statement for months. Affinion, Webloyalty, and Vertrue have all denied any wrongdoing and argue that their services offer users savings and are valued by many subscribers.
Source: http://news.cnet.com/8301-1023_3-10399028-93.html

14. *November 16, Reuters* – (National) **SEC files charges over "green" Ponzi Scheme.** The U.S. Securities and Exchange Commission (SEC) charged four individuals and two companies with running a $30 million Ponzi scheme that targeted elderly investors and people nearing retirement who were seeking environmentally friendly investments. In a civil lawsuit filed on November 16 in Denver federal court, the SEC accused Mantria Corp of Bala Cynwyd, Pennsylvania and its principals of raising $122 million from more than 300 investors nationwide in a dozen fraudulent

securities offerings. The SEC said Mantria enlisted Speed of Wealth LLC, a Centennial, Colorado firm and its owners, to encourage investors to liquidate retirement plans and home equity, and buy securities offering returns of 17 percent to "hundreds of percent" annually. It said the owners of Speed of Wealth encouraged victims through seminars, the Internet and phone calls "to move at the speed of wealth" to invest in Mantria's securities, receiving a 12.5 percent commission for their efforts. According to the SEC, Mantria purported to use the securities to finance such projects as a "carbon negative" housing community in rural Tennessee, and production of "biochar," a charcoal substitute made from organic waste. Instead, it said Mantria overstated its own investment success, and used much of the proceeds from new investments to repay earlier investors. The SEC charged Mantria, Speed of Wealth, and the four individuals with fraud and the sale of unregistered securities. It is seeking the return of illegal profits, civil fines, and a freezing of the defendants' assets.
Source: http://www.reuters.com/article/GCA-GreenBusiness/idUSTRE5AF50W20091116

[Return to top]

Transportation Sector

15. *November 17, Associated Press* – (Massachusetts) **Passenger removed from trans-Atlantic flight.** A U.S. Airways airliner en route from Philadelphia to London made an unscheduled stop in Boston Monday after the pilot deemed a passenger's behavior unruly and decided to have him removed from the plane. A Glasgow, Scotland man was arrested shortly after flight 728 landed at Logan International Airport on Monday, said an airport spokesman. The plane departed for London two hours later, the spokesman said. The Glaswegian was being held in Boston early Tuesday. The airport spokesman said he was arrested for interfering with a flight crew. It was not clear if he had been charged, and police were not immediately available for comment. A U.S. Airways spokesman said the pilot decided to land the plane in Boston and have the man removed before beginning the trans-Atlantic crossing "in the interest of safety."
Source: http://www.foxnews.com/story/0,2933,575370,00.html?test=latestnews

16. *November 17, Denver Post* – (Colorado) **Deteriorating concrete closes bridge over South Platte River.** The Colorado Department of Transportation (CDOT) on Monday closed the bridge that takes East 104th Avenue over the South Platte River after engineers discovered significant deterioration of concrete on key portions of the structure. Traffic will be detoured to East 88th Avenue, a CDOT spokeswoman said. Repairs are expected to begin in about three weeks, and the fix may take another two weeks to complete, she said.
Source: http://www.denverpost.com/news/ci_13803766

17. *November 16, Associated Press* – (Virginia) **Crews set to tow runaway barge.** A runaway barge pushed by a violent storm into the surf off of Virginia Beach is ready to be towed off to sea. The Coast Guard says the 570-foot vessel could be towed from the Sandbridge section of the resort city sometime on November 16. A spokesman for the

shipping company that owns the barge says the vessel has empty containers with possible chlorine residue. The guard says there is no evidence the barge has leaked. Since the barge drifted perilously close to the fishing pier on Friday, onlookers have gathered to look at the wayward ship. The barge was being towed from San Juan, Puerto Rico to New Jersey when a cable snapped, freeing the barge.
Source: http://www.wric.com/Global/story.asp?S=11511355

18. *November 16, Torrance Daily Breeze* – (California) **Report: LAX taxiway modifications would improve safety.** The relocation of two high-speed taxiways and the construction of a third taxiway on the north airfield may improve safety at Los Angeles International Airport, according to a report released Monday. The Board of Airport Commissioners is expected to review the $50 million proposal in the next several months, but construction would not likely begin until September 2011, pending approval from the Federal Aviation Administration, said the executive director of LAX. "We are not suggesting that this fixes stuff up there," the director said. "It would just make things a little less hazardous or a little less catastrophic if they are moved. We're under no circumstances finished and we have a lot of work to do." In February, NASA Ames Research Center is expected to announce the results of a $1.4 million study aimed at determining whether the north airfield's two parallel runways should be separated to make room for a centerline taxiway, similar to a project completed last year at the airport's south airfield.
Source: http://www.dailybreeze.com/news/ci_13800631

For more stories, see items **2**, **4**, and **6**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

19. *November 17, KCCI 8 Des Moines* – (Iowa) **Workers hurt in Iowa grain blast.** Two workers were hurt Monday morning during an explosion at a grain elevator in northern Iowa. A spokesperson for West Central Cooperative, said the small explosion came from a grain dryer near the Boxholm elevator around 8:45 a.m. Two employees nearby were hurt in the blast, one was working on a platform on the grain dryer at the time of the explosion. The spokesperson said the worker's injuries are believed to be non-life threatening. She said one was treated and released from the hospital. The other worker was still being evaluated as of noon on Monday. The cause of the explosion remains under investigation. A couple hours after the blast, smoke could still be seen coming from the dryer area. Crews are expected to wrap up their work this afternoon, but officials said the elevator would likely remain closed until mid-week. Farmers will be

directed to other nearby elevators until the Boxholm Co-op can reopen. Fire crews at the scene said the incident is the fourth time this fall they have been called to a fire involving a grain dryer. Crews worked to remove the grain from the dryer to help put out the fire.
Source: http://www.firehouse.com/topics/rescue-and-special-ops/workers-hurt-iowa-grain-elevator-blast

20. *November 16, XETV 6 San Diego* – (California) **Bomb scare at Fallbrook grocery store.** The discovery of an object resembling a pipe bomb in a restroom at a Fallbrook, California grocery store prompted an evacuation of the business Monday afternoon. A caller reported finding the suspicious-looking cylinder inside the market in the 1100 block of South Main Street at about 1:30 p.m., according to sheriff's officials. Bomb-arson personnel were sent to the scene to investigate. The incident had been safely resolved by 5 p.m., according to a police lieutenant, it was not immediately clear if the object was actually a home-made explosive device or just something that resembled one. No injuries were reported, she said.
Source: http://www.sandiego6.com/news/local/story/Bomb-Scare-at-Fallbrook-Grocery-Store/Q3tmO8v9eUS7VzBEefon9g.cspx

[Return to top]

Water Sector

21. *November 16, Albany Times Union* – (New York) **Old sewer pipes creating a tough challenge.** Aging sewer systems in the Capital Region of New York are dumping more than a billion gallons of watered-down, untreated sewage into the Hudson River each year, according to a report by the Capital District Regional Planning Commission (CDRPC). The first-ever report on river pollution caused by sewers that serve more than 150,000 people also warned that repairs to keep sewage out of the river will be incredibly expensive, likely in the hundreds of millions of dollars. The river is under assault from 1.2 billion gallons of "combined sewer overflows" annually from systems in Albany, Troy, Watervliet, Rensselaer, Cohoes, and the village of Green Island, said the director of the CDRPC. Overflows happen more than 230 times each year, for a total of more than 1,900 hours, or the equivalent of 80 days a year, according to the CDRPC report. Each spill lasts for about eight hours on average. Required before the U.S. Environmental Protection Agency would issue continued water pollution permits for the local sewer districts, the report took four years to complete. Now, another year's worth of study is planned to come up with proposed repairs and an estimated price tag. Repairs could involve adding capacity to sewer treatment plants, and changing how rainwater is handled so less reaches storm drains, possibly by "green infrastructure" such as plantings and green roofs that direct more water to be reabsorbed into the ground.
Source: http://www.timesunion.com/AspStories/story.asp?storyID=866190

22. *November 16, Davidson County Dispatch* – (North Carolina) **Thomasville reports wastewater spill.** The City of Thomasville, North Carolina, had four untreated

wastewater spills of an estimated total of 65,000 gallons during the heavy rains Wednesday and Thursday. The first three spills were from man holes and the fourth from a sewage pumping station. The first spill of approximately 10,000 gallons was near the corner of Warner and Julian streets. The second spill was also approximately 10,000 gallons at Franklin Street. Both of these spills entered tributaries to Hanks Branch Creek. The third spill, also estimated at approximately 10,000 gallons, was from a manhole on Concord Street and entered the North Hamby Creek. The fourth spill, estimated at 35,000 gallons, occurred at the East Davidson Pump Station on Old Emmanuel Church Road and entered South Hamby Creek. All four spills occurred in and entered the Yadkin/Pee Dee River Basin. The Division of Emergency Management was notified of the spill Tuesday and is reviewing it. State law requires municipalities, animal operations, industries and others who operate waste-handling systems issue a news release when a spill of 1,000 gallons or more reaches surface waters.
Source: http://www.the-dispatch.com/article/20091116/ARTICLES/911169992/1005/NEWS?Title=Thomasville-reports-wastewater-spill&tc=autorefresh

For another story, see item **29**

[Return to top]

Public Health and Healthcare Sector

23. *November 16, U.S Food and Drug Administration* – (National) **FDA approves additional vaccine for 2009 H1N1 influenza virus.** The U.S. Food and Drug Administration (FDA) announced that it has approved a fifth vaccine for protection against the 2009 H1N1 influenza virus. The vaccine is manufactured by ID Biomedical Corp. of Quebec, Canada, owned by GlaxoSmithKline, PLC. As with the four previous H1N1 influenza vaccines licensed by the FDA on September 15, 2009, ID Biomedical Corporation will manufacture its H1N1 vaccine using the established, licensed egg-based manufacturing process used for producing seasonal flu vaccine. Potential side effects of this H1N1 vaccine are expected to be similar to those of the seasonal and H1N1 flu vaccines. The most common side effect is soreness at the injection site. Others may include mild fever, body aches and fatigue for a few days after the inoculation. As with any medical product, unexpected or rare serious adverse events may occur. The FDA is collaborating with other government agencies to enhance adverse event safety monitoring during and after the H1N1 2009 vaccination program. ID Biomedical's H1N1 monovalent vaccine will be produced in multi-dose vials, in a formulation that contains thimerosal.
Source: http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm190783.htm

24. *November 16, DarkReading* – (National) **Conn. AG investigates Blue Cross Blue Shield data breach.** Connecticut's attorney general (AG) is investigating Blue Cross Blue Shield's loss of confidential information, including tax identification and Social Security numbers, for 800,000 healthcare providers nationwide. The attorney general is

also seeking additional identity theft protection for affected doctors, therapists, and other professionals, according to a statement from the attorney general issued last week. Blue Cross Blue Shield and its affiliates "may have violated state law by losing the information and failing to notify providers in a timely manner," the AG said. The companies are offering professionals one year of identity theft protection, but the AG said the measures ere "inadequate and unacceptable," demanding at least two years of protection. Anthem Blue Cross and Blue Shield, one of the targeted companies, said it will extend credit monitoring to two years for affected providers. The companies lost the information when a laptop was stolen August 25. The computer held information on the companies' providers nationwide, including names, addresses, tax identification and provider numbers, and some Social Security numbers. The theft affected providers nationwide, but the Connecticut AG is investigating on behalf of 18,817 of its Connecticut health care providers.
Source:
http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=221800146&cid=ref-true

25. *November 16, Register* – (International) **Spammers aim to profit from swine flu pandemic.** Russian cybercrooks have laid the groundwork needed to build a business cashing in on swine flu panic-buying. Tamiflu sales from dodgy unlicensed pharmaceutical websites are being promoted through spam email, search engine manipulation and a variety of other underhand techniques. Web affiliates, commonly based in Russia where they are called Partnerka, are driving traffic to dodgy pharmaceutical sites using a variety of spam and adware-related marketing tactics. Hundreds of virtually similar so-called "Canadian pharmacy" sites exist. Although they claim to be based in Canada, (a tactic designed to add a thin layer of legitimacy) the sites might be actually be located anywhere in the world. Sophos reports that members of Glavmed, one of the more popular Russian affiliate networks, can earn an average of $16,000 a day promoting such dodgy pharmacy websites. These sites have begun advertising Tamiflu alongside more traditional products such as Viagra and Ciallis. Responding to these "spamvertised" websites risks exposure to potentially dangerous drugs, while also handing over personal data to cybercrooks, net security firm Sophos warns. This July witnessed a huge increase in UK internet searches for Tamiflu, at a time when concerns that global Tamiflu production was falling behind schedule. The northern winter could see a repeat of this interest, creating a demand that unlicensed online pharmacies are ready to exploit.
Source: http://www.theregister.co.uk/2009/11/16/swine_flu_spam/

26. *November 16, Wicked Local Brookline* – (Massachusetts) **Brookline hospital building flooded after patient damages sprinkler.** Brookline, Massachusetts, firefighters were called to Bournewood Hospital in South Brookline around 9:30 p.m. November 13 after a patient reportedly ripped off an emergency sprinkler head and sent water gushing through the building. The fire chief said the flood caused water damage to all three floors of the Stedman Building, which houses administrative offices and an adult psychiatric unit. He said the damaged sprinkler was in a second-floor bathroom. The Brookline Fire Department was automatically notified when the sprinkler system was

triggered. Three companies responded to the hospital and remained there for about 20 minutes while shutting off the sprinkler.
Source:
http://www.wickedlocal.com/brookline/news/police_and_fire/x687825471/Brookline-hospital-building-flooded-after-patient-damages-sprinkler

[Return to top]

Government Facilities Sector

27. *November 16, KTRK 13 Houston* – (Texas) **Suspicious device found at city hall.** A suspicious device was found outside Surfside's City Hall on November 16. Investigators say the device was not dangerous, but it was suspicious enough to keep city hall shut down for most of the morning. A water clerk for the City of Surfside had come outside to smoke a cigarette. But when she tried to dispose of her cigarette butt in a special ashtray, she found a device had been jammed inside. To the naked eye, the device looked like it could be a pipe bomb. The Surfside Police Department initially treated it as such. There were seven people inside the city hall and police building at the time. Those people were evacuated. The local sheriff's department was called out. They, in turn, summoned the FBI. FBI officials removed the device from the ashtray and evaluated it, determining it was some sort of device that is routinely used by telephone companies. They said while it appeared more dangerous than it was, an investigation is still ongoing. Authorities are reviewing surveillance camera video to determine who may have been behind the prank. It's believed the device was placed in the ashtray sometime between 5pm Friday and 7:30am Monday, when it was discovered. No one was injured, and all employees were back at work by lunchtime.
Source: http://abclocal.go.com/ktrk/story?section=news/local&id=7121665

28. *November 16, WFMY 2 Greensboro* – (North Carolina) **Sheriff: Gang member threatened mass shooting at community college.** Investigators say an 18-year-old was arrested after threatening to do a "mass shooting" at Alamance County Community College. The suspect, an alleged member of street gang "Neighborhood Mafia," turned himself in to Burlington Police on Saturday after warrants were issued for his arrest. Alamance County Sheriff's Office began investigating the suspect after a teacher at the Middle College reported being threatened. The suspect is charged with Feloniously Making a False Report of Mass Violence on Education Property and Misdemeanor Communicating Threats. He is being held in the Alamance County Jail under a $100,000 bond.
Source: http://www.digtriad.com/news/local/story.aspx?storyid=133233&catid=57

29. *November 15, Honolulu Adverstiser* – (Hawaii) **Heavy rains disrupt water service in parts of Kauai, closes Hanalei school.** State education officials have closed the Hanalei Elementary School because of the water disruption in the area and portions of Wailua Houselots because of heavy rains and flooding, Kauai County officials said November 14. In addition, residents who live on Waipouli and Hauiki roads in the Wailua-Kapa'a area should boil their water before using it because of the possible

contamination caused by infiltration from surface water due to the heavy rains, county officials said. Fecal coliform or E coli bacteria could possibly be in the water, which might cause diarrhea, cramps, nausea, headaches, or other symptoms, officials said. The halt in water service also required state Department of Education officials to announce the closure of the Hanalei Elementary School today. Flyers were passed out door-to-door earlier yesterday by county Department of Water officials warning affected residents of the possible contamination.
Source: http://www.honoluluadvertiser.com/article/20091116/BREAKING01/311160017/Heavy+rains+disrupt+water+service+in+parts+of+Kauai++closes+Hanalei+school+

30. *November 15, KOLD 13 Tucson* – (Arizona) **Protestors arrested at Ft. Huachuca.** A protest at Fort Huachuca Sunday resulted in the arrest of five people for trespassing. A Fort Huachuca spokesperson confirmed to KOLD News 13 that the five were detained for about an hour and then released. The military has officially banned them from the base for a year. The group alleges that Fort Huachuca continues to train soldiers in torture interrogation techniques, which they claim have been used in places like Guantanamo Bay. Earlier, they held a vigil and marched to the Main Gate at Fort Huachuca. The U.S. Army has maintained that training at the Fort abides by U.S. laws and is conducted in a transparent manner.
Source: http://www.kold.com/Global/story.asp?S=11510289

31. *November 15, Topeka Capital Journal* – (Kansas) **Cold War missile site targeted.** Though the weapons have long since been removed and the collective eyes of the world no longer concern themselves with the day-to-day operations, missile sites in Kansas from the Cold War continue to elicit careful attention from the Army Corps of Engineers. This is because more than bygone flashes of history can be found at some of the sites. A chemical agent called trichloroethylene (TCE) was used as a degreasing agent to clean fuel lines to ensure missiles at the sites were operationally ready and able to fire on cue. Workers did not think twice about dumping the chemical on-site. However, since that time it has been discovered the chemical can have dangerous health effects at high levels. There are 21 former Atlas missile sites and five former Nike missile sites in Kansas that are part of the Formerly Utilized Defense Sites program sponsored by the Department of Defense to evaluate and remediate contamination at formerly used defense sites (FUDS). The primary contamination is TCE in groundwater and soil. The corps is responsible for management and execution of the FUDS program.
Source: http://cjonline.com/news/local/2009-11-14/cold_war_missile_site_targeted

[Return to top]

Emergency Services Sector

32. *November 17, Sandusky Register* – (Ohio) **Erie County getting 911 backup cable.** Erie County's Emergency Management Agency (EMA) has endured hours-long outages of its 911 system on two occasions in recent months. Nonetheless, the agency

seems to have learned. It is shelling out $7,400 to install a backup cable for Erie County's 911 system. County commissioners on Thursday approved the EMA director's request to install the communications cable, which will serve as a backup in the event anything happens to the primary 911 lines. "Based on the problems we had these past two months with 911 ... it would behoove us to move forward as quickly as possible," said the county commissioner. The county's 911 system was down for hours August 23 when county workers shredded a phone cable while rototilling a garden near the county services building on Columbus Avenue. Not a month later, private contractors digging a trench near the same building snagged a 911 cable with the bucket of a backhoe. That knocked out 911 service for the better part of seven hours. The backup cable will create something of a fallback in the event anything else goes wrong, county officials said. "With this configuration, if one of these cables might be damaged in the future, we would have a redundant system to route calls through," the EMA director wrote in a November 9 letter to commissioners.
Source: http://www.sanduskyregister.com/articles/2009/11/17/front/1738174.txt

33. *November 16, Associated Press and Charleston Gazette* – (West Virginia) **Apparent power surge forces Metro 911 to new backup site.** Last week, Kanawha County, West Virginia officials practiced moving Metro 911's operations to a secondary Public Safety Answering Point, a backup site where 911 calls are handled if something catastrophic happens at the Ned Chilton Metro 911 call center. On Monday, the backup facility was put to the test. A freak power outage at the Metro 911 center at Southridge forced county officials to move their emergency operations, including the fielding of 911 calls and communications for police, fire and ambulance services, to the backup location for almost two hours. Around 11:30 a.m., computers in the command center suddenly went black, said Metro 911's director. Within moments, the supervisor began transferring operations to the backup facility, located within another county agency. The cause of the outage was not known on Monday, but Kanawha's county commission president said he thinks it was a significant power surge. The surge might have caused the facility's uninterrupted power system to trip a number of breakers, cutting power to vital parts of the building.
Source: http://wvgazette.com/News/200911160406

34. *November 16, CNET News* – (California) **Hackers use tech to solve disaster relief challenges.** Last week at the Hacker Dojo in Mountain View, California, developers partnered with Google, Yahoo, NASA, and the World Bank to exchange ideas and work on solutions for responding to natural disasters and other emergencies. Random Hacks of Kindness is the first in a series of planned events that seek to use technology to solve real world problems related to crisis and disaster relief. By first working with governments and non-governmental organizations to better understand the immediate needs of rescuers and communities following a critical emergency, these programmers are work directly to solve communication issues and to better facilitate the exchange of information and resources in times of need. Often, information comes from a wide array of sources during emergencies, including governments, rescuers, and victims in local communities. Successfully organizing the incoming content and delivering

information back to the proper resource is a critical part of providing aid to victims.
Source: http://news.cnet.com/8301-30252_3-10399130-246.html

35. *November 16, WSAZ 3 Huntington* – (West Virginia) **Cell phones changing how emergency responders work.** While using only cell phones can be cheaper and more convenient, it is also changing the way emergency responders do their jobs. Kanawha County is among counties throughout our region working to keep up with the changing times. As technology advances, the way residents find out about emergencies is constantly changing, too. The folks at Metro 911 in Kanawha County are asking county residents to be proactive about providing their cell phone numbers and e-mail addresses. That is so that when a wide scale emergency happens, 911 officials can tell you faster and more directly. In some cases, the system would zone in on people in a certain area. But when problems hit that are countywide, everyone would get the alert.
Source: http://www.wsaz.com/news/headlines/70239592.html

[Return to top]

Information Technology Sector

36. *November 17, Network World* – (International) **Are nations paying criminals for botnet attacks?** Nations that want to disrupt their enemies' banking, media and government resources can simply order botnet attack services from cybercriminals. In McAfee's new report, "Virtually Here: The Age of Cyber Warfare," draws from the opinions of about 20 experts, including a former deputy director of the U.S. National Security Agency. U.S. cyber war policy needs new focus, experts say. There have been several larger denial-of-service attacks over the past few years that raised suspicions about whether they were initiated by nations in conflict against their adversaries. Such incidents include cyberattacks that hit Estonia and Georgia, which some viewed as traceable to Russia. More recently, many were tempted to blame North Korea for this year's July 4th cyberattacks on South Korea and U.S. resources. The McAfee report, prepared by an analyst at Good Harbor Consulting, presents the opinions of diplomats, researchers and others about the nature of cyberattacks that seem concentrated on a specific country but where it's hard, if not impossible, to determine whether or not another nation-state initiated the attack. One reason it may be hard to tell is simply because a nation state may go to the criminal underground to secretly pay for a massive botnet attack against its enemy. In this case, it is conceivable that the criminals themselves would not fully understand what they are being asked to do since the request and payment of botnet attack services are typically carried out as anonymously as possible, says the vice president of threat research at McAfee.
Source:
http://www.computerworld.com/s/article/9141000/Are_nations_paying_criminals_for_botnet_attacks_

37. *November 16, Register* – (International) **DNSSec update deadline penciled in for 2011.** VeriSign announced plans on November 16 to roll out the DNSSec security standard for the web's .com and .net Top Level Domain Names (TLDs) by the first

quarter of 2011. Short for Domain Name System Security Extensions Protocol, DNSSec is designed to guard against "man in the middle" and cache poisoning attacks that create a means for hackers to hijack web browsing sessions. DNSSec adds digital signature to domain name requests, thus making the system more secure. The technology has existed for more than a decade but it was only after a researcher discovered a block-buster DNS flaw last year that anybody started paying serious attention to architectural shortcomings that have plagued the net's domain name system since its very beginning. A decision by the U.S. government to move .gov domains from vanilla DNS to the more secure DNSSec last year began the long-awaited migration process, which has finally begun to get moving after years of technical and bureaucratic problems. VeriSign has begun working with EDUCAUSE, the association for information technology in higher education, and the Department of Commerce to deploy DNSSec within the .edu TLD. Lessons learned from this process will be applied to the bigger job of introducing DNSSec to the .net and .com domains over the next 18 months or so.
Source: http://www.theregister.co.uk/2009/11/16/dnssec_roll_ou/

38. *November 16, DarkReading* – (International) **Most security products don't initially work as intended, study says.** Nearly 80 percent of security products fail to perform as intended when first tested — and most require two or more cycles of testing before achieving certification, according to a new report from ICSA Labs, which performs security product testing. The ICSA Labs Product Assurance Report — a first-of-its-kind study co-authored by ICSA and the Verizon Business Data Breach Investigations Report research team — offers insights from ICSA's tests of thousands of security products from the past 20 years. According to the report, the main reason why a security product fails during initial testing is that it does not adequately perform as intended. Across seven product categories, core product functionality accounted for 78 percent of initial test failures — for example, an antivirus product failing to prevent infection or an intrusion prevention system product failing to filter malicious traffic. The failure of a security product to completely and accurately log data was the second most common reason for test failure, according to the report. Fifty-eight percent of failures were attributed to incomplete or inaccurate logging of who did what — and when, ICSA said. The report findings suggest some vendors and enterprise users consider logging a nuisance. According to the report, logging is a particular challenge for firewalls. Almost every network firewall (97 percent) or Web application firewall (80 percent) tested by ICSA experienced at least one logging problem. The third most significant reason for test failure was inherent security problems in the products themselves, including vulnerabilities that compromise the confidentiality or integrity of the system, ICSA said. The product categories studied were antivirus, network firewall, Web application firewall, network IPS, IPSec VPN, SSL VPN, and custom testing.
Source: http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=221800221

39. *November 16, Albany Legislative Gazette* – (National) **NY gets $3M. to help stop cyber attacks.** New York state has secured $3 million in federal funding to help protect

state and local government computer networks against cyber attacks. The funding is part of the 2010 Department of Homeland Security Appropriations Act, which the President signed on October 28. The $3 million will facilitate New York's cyber security efforts through the Multi-State Information Sharing and Analysis Center, which is operated by the state Office of Cyber Security and Critical Infrastructure Coordination. The federal appropriation will also enable the organization to make program enhancements such as real-time threat detection and prevention for more state, local, and territorial governments. The center is focused on cyber threat prevention, protection and response and recovery for state, local and territorial governments across the country and serves as a lookout for cyber security threats. It now oversees all Los Angeles airports as well. It looks for threats to governments around the country by identifying both the causes and vulnerabilities. "Most people don't see this," said the director of the Office of Cyber Security and Critical Infrastructure Coordination. "Other than weapons of mass destruction, cyber security is of the most concern." Cyber terrorists and thieves could conceivably take control of the electric grid or steal from banks, agencies or individuals, he said. They could also, for example, get control of flood gates for dams, which could cause as much damage as a bomb. He said he does not know exactly when the money will be administered but said it will be distributed to state and local governments and used to beef up monitoring when it arrives. "We are it for the country right now," said the director. "This is real. We're being attacked everyday."
Source: http://www.legislativegazette.com/Articles-c-2009-11-16-63976.113122_NY_gets_3M_to_help_stop_cyber_attacks.html

For more stories, see items **25** and **34**

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Website: http://www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/.

[Return to top]

Communications Sector

40. *November 17, Product Reviews News* – (International) **BlackBerry Outage: Internet service hit again.** We have heard reports that BlackBerry users have been suffering from another internet outage, mainly the BlackBerry Internet Service (BIS), which is possibly affecting customers all around the world. Around 75-80% of BlackBerry users have been affected by the problem, and it is not just targeting specific carriers either.
Source: http://www.product-reviews.net/2009/11/17/blackberry-outage-internet-service-hit-again/

41. *November 16, Christian Science Monitor* – (National) **ATT net service halted by cut fiber cable.** Access to AT&T's webmail was interrupted Monday morning because a fiber optic cable was disabled. The service was working again by 10:15 a.m. E.S.T. "Due to a fiber cut, access to www.att.net was temporarily impacted earlier this morning," a company spokesman wrote in an e-mail. "Access to the att.net site has been restored." The outage cut off users from their AT&T Web-based e-mail and other services for several hours. Some AT&T users reported difficulties last night as well, according to a news report.
Source: http://features.csmonitor.com/economyrebuild/2009/11/16/att-net-service-halted-by-cut-fiber-cable/

For more stories, see items **12**, **32**, **33**, and **35**

[Return to top]

Commercial Facilities Sector

42. *November 17, KRMG 740 AM Tulsa* – (Oklahoma) **Three buildings evacuated at Owasso apartment complex after pipe bomb is found, man arrested.** A search warrant for a drug suspect yesterday turned up a pipe bomb along with the alleged marijuana. The Tulsa Police Bomb Squad was called after Owasso Police found the bomb in a closet at the Greens Apartments. The device was disabled at the scene near 86th Street North and 145th East Avenue. An Owasso deputy police chief did not identify the suspect who was taken to jail for drug possession. He says the suspect also could face federal charges for building a pipe bomb.
Source: http://krmg.com/localnews/2009/11/three-buildings-evacuated-at-o.html

43. *November 16, Macon Sun* – (Georgia) **Fire burns warehouse of Ken's Stereo Junction.** Several dozen televisions burned up in a warehouse fire this morning at Ken's Stereo Junction on Mercer University Drive. The Macon-Bibb County Fire Department Captain said heavy smoke was showing from the building at about 6:50 a.m. when the call came in to the 911 center. Firefighters were able to save the building by knocking the fire out in less than 30 minutes but about half the contents of the metal warehouse was destroyed or damaged by fire. They moved some of the merchandise and protected it from the flames, he said. The business's owner said 60 to 70 large televisions were destroyed in the blaze that appears to have been sparked by a faulty heater. A stack of televisions that nearly reached the ceiling in the one-story building had been melted down to about three feet high. The westbound lane of Mercer University Drive was blocked by fire hoses for about three hours as crews put out the fire and investigated the cause.
Source: http://www.macon.com/breaking_news/story/918721.html

For another story, see item **20**

[Return to top]

National Monuments and Icons Sector

44. *November 17, Associated Press* – (West Virginia) **Arson suspected on West Virginia park land.** Officials believe arson was the cause of a fire on land in West Virginia that's part of the New River Gorge National River property. According to a park ranger, the four-acre fire was reported near Bragg on the afternoon of November 15. Crews worked through the evening to put out the blaze. He added that some hot spots remain, and firefighters plan to be on the scene Monday to fully extinguish them. No structures were damaged and no one was injured. National Park Service investigators are still looking into the fire, but suspect it was deliberately set.
Source: http://www.claimsjournal.com/news/southeast/2009/11/17/105378.htm

[Return to top]

Dams Sector

45. *November 16, KING 5 Seattle* – (Washington) **Corps finishes interim Howard Hanson Dam repairs.** The U.S. Army Corps Engineers says contractors have wrapped up what it calls interim risk reduction measures on the Howard Hanson Dam. The main feature of that work was the so called "grout curtain". Contractors pumped thousands of gallons of a cement mixture into the earthen section of the dam. The grout finds and fills gaps and crevices which led to dangerous levels of seepage earlier this year. The Corps still warns it will not allow the dam to fill up to its normal levels this winter, which may mean some flooding along the Green River. Recent steady rain storms have them carefully monitoring the river above and below the dam, but they say there is no risk of flooding at this point. The Corps is much more concerned about relentless rains pounding the Kitsap Peninsula and the forecast calls for more of the same. The Corps has assumed control of the Wynoochie River Dam north of Aberdeen and has activated its flood center, meaning it will be staffed around the clock until rain and river levels go down.
Source: http://www.king5.com/news/local/Corps-Finishes-Howard-Hanson-Dam-Repairs-70227757.html

46. *November 16, Eugene Register-Guard* – (Oregon) **EWEB shuts down Walterville canal after small leak reported.** The water level in a four-mile stretch of the lower McKenzie River in Oregon, is expected to be higher than normal for the next day or so because of the unexpected shutdown of the Eugene Water and Electric Board's (EWEB) Walterville Power Canal late Monday afternoon, utility officials said. EWEB closed off water diversion from the McKenzie into the canal as a precautionary measure about 4 p.m., after a neighbor living near the Walterville Powerhouse reported water leaking from the canal onto his property. The precautionary shutdown leaves the full amount of water in the McKenzie from the canal intake east of Walterville to the outflow below the powerhouse. The river level on Monday evening was about 3,900 cubic feet per second. The small water leak stopped when the canal level dropped by about 2 feet by early Monday evening, EWEB said. The utility plans to inspect the canal further during daylight hours today and will perform repairs as needed.

Source: http://www.registerguard.com/csp/cms/sites/web/updates/23199713-55/story.csp

[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 Website: http://www.dhs.gov/iaipdailyreport

Contact Information

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

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer