



## Department of Homeland Security Daily Open Source Infrastructure Report for 24 November 2008

Current Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)  
<http://www.dhs.gov/>

- Bloomberg reports that Delek U.S. Holdings Inc. temporarily halted production at its Tyler, Texas, refinery after an explosion and fire Thursday that killed one worker. (See item [1](#))
- According to the Associated Press, Federal Bureau of Investigation officials said Friday they arrested a man who allegedly threatened to blow up the Paul Brown Stadium in Ohio and other area landmarks. (See item [36](#))

### DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: [Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams](#)

Service Industries: [Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities](#)

Sustenance and Health: [Agriculture and Food; Water; Public Health and Healthcare](#)

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. *November 21, Bloomberg* – (Texas) **Delek halts production at Texas refinery, worker dies.** Delek U.S. Holdings Inc. temporarily halted production at its Tyler, Texas, refinery after an explosion and fire Thursday that killed one worker, the company said in a statement on its Web site. The blast occurred at approximately 2 p.m. in the saturates gas plant at the Texas refinery, a separate statement from the unit of Israeli holding company Delek Group Ltd. showed. “There has been one fatality resulting from a fire,” the company said. “The cause of the incident and the extent of the damage to the refinery have not yet been established.” The man died overnight after being airlifted to a medical center with burn injuries, KLTV reported. At least six workers were provided medical treatment after the blast.

Source:

<http://www.bloomberg.com/apps/news?pid=20601207&sid=aPLg0oSgt8W8&refer=energy>

2. *November 20, Denver Post* – (Colorado) **Power plants to track mercury.** The Colorado Air Quality Control Commission on Thursday approved a requirement for systematic monitoring of mercury emissions from power plants starting January 1. The monitoring is the first part of a state rule requiring an 80 percent cut in mercury emissions by 2014 and a 90 percent reduction by 2018. The vote puts Colorado among a handful of states, including Connecticut and Arizona, with rules to control power-plant mercury emissions. Under the Colorado regulation, power plants will begin monitoring their mercury emissions and report them to the state Air Pollution Control Division. Eleven plants come under the rule. The larger ones will use continuous monitors, and the smaller ones will do periodic stack tests. By 2012, Xcel Energy's Pawnee plant and the Platte River Power Authority's Rawhide plant will cut their emissions by 80 percent. All other plants will face a 2014 deadline to cut emissions by 80 percent. "Pawnee and Rawhide are two of the biggest plants in the state, and they voluntarily agreed to go first," said the division's manager for stationary sources. The rule had no opposition because of negotiations among key parties, said a lawyer with the Boulder office of the Environmental Defense Fund.  
Source: [http://www.denverpost.com/headlines/ci\\_11036508](http://www.denverpost.com/headlines/ci_11036508)

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

## **Chemical Industry Sector**

3. *November 21, Associated Press* – (Oklahoma) **2 businesses evacuated after acid leak.** Authorities say two businesses in northeast Oklahoma City had to be evacuated after a liquid muriatic acid leak. The Fire Battalion Chief on the scene said the leak yesterday afternoon at Chemstation didn't cause any injuries. The Chemstation building and a business to the west were evacuated. According to the fire chief, a 275-gallon canister leaked about 50 gallons of the acid about 2:30. The acid spilled inside the Chemstation building and into the parking lot.  
Source: <http://www.kfsm.com/Global/story.asp?S=9390922>

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

## **Nuclear Reactors, Materials, and Waste Sector**

4. *November 21, Reuters* – (Alabama) **Southern Ala. Farley 1 reactor exits outage.** Southern Co.'s Unit 1 at the Farley nuclear power station in Alabama exited an outage and ramped up to 69 percent by early Friday, the U.S. Nuclear Regulatory Commission said in a report. The unit automatically tripped on November 19 due to a low voltage indication in the switchyard. To protect itself from damage, equipment at the plant is programmed to shut automatically on low voltage indications.  
Source:  
<http://www.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUSN2145897220081121>

5. *November 21, Washington Post* – (Maryland) **Coalition challenges proposed 3rd reactor.** A coalition of environmental organizations filed legal challenges last week against the proposed third nuclear reactor at Calvert Cliffs. The group told the U.S. Nuclear Regulatory Commission (NRC) that the problems with UniStar Nuclear Energy’s application to build a reactor at the Lusby site include the concurrent review of the reactor design and the license application; the storage and disposal of radioactive waste; and foreign partnerships involved in the project. “We are basically trying to point out the inadequacy of the application itself. The issues we are raising will demonstrate that this is both an economically and environmentally bad deal for Maryland,” said the energy organizer for Public Citizen’s Energy Program. “We believe we have picked the safest and most secure new nuclear technology that exceeds federal standards for safety and the protection of the public as well as enhancing U.S. energy security,” said a spokeswoman for Constellation Energy, which is a partner with a European energy company in UniStar. The agency will review the filings in the next months and determine whether they are legally admissible, said an NRC spokesman.  
Source: [http://www.washingtonpost.com/wp-dyn/content/article/2008/11/20/AR2008112003596.html?nav=rss\\_metro](http://www.washingtonpost.com/wp-dyn/content/article/2008/11/20/AR2008112003596.html?nav=rss_metro)
  
6. *November 20, U.S. Nuclear Regulatory Commission* – (Kansas) **NRC approves license renewal for Wolf Creek nuclear power plant for an additional 20 years.** The U.S. Nuclear Regulatory Commission (NRC) has approved the operating license renewal of the Wolf Creek Generating Station in Kansas for an additional 20 years. The operator, Wolf Creek Nuclear Operating Corp., submitted its license renewal application September 27, 2006. With the renewal, the license is extended until March 11, 2045. The NRC’s environmental review for this license renewal concluded there were no environmental impacts that would preclude renewal of the license for environmental reasons. After carefully reviewing the plant’s safety systems and specifications, the staff concluded that there were no safety concerns that would preclude license renewal, because the applicant had effectively demonstrated the capability to manage the effects of plant aging.  
Source: <http://www.nrc.gov/reading-rm/doc-collections/news/2008/08-213.html>

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

## **Defense Industrial Base Sector**

7. *November 20, Associated Press* – (National) **Car makers say bailout a defense issue.** In an increasingly anxious campaign for a \$25 billion government rescue, Detroit’s Big Three car makers and their allies in Washington are warning the demise of the auto industry will damage U.S. national security. That argument is a hard sell. General Motors Corp., Ford Motor Co. and Chrysler LLC long ago exited the defense business. While many of their suppliers also make the parts used on military vehicles and would be hit by the wave if one of the Big Three collapsed, defense experts see little immediate risk to the Armed Forces beyond paying higher prices. “It’s a stretch, quite frankly,” said a retired Army Lieutenant General, chairman of the National Defense Industrial Association’s combat vehicles division. “I think they are grasping at straws.” While

acknowledging that the defense market is largely separate from the auto industry, proponents say that the defense market alone is not large enough to sustain most auto parts suppliers, making a strong commercial industry key to their survival. Additionally, some point to the success of the MRAP armored truck in Iraq as an indicator of the necessity of saving the Detroit automakers. But the Big Three had no role in making the hulking MRAPs, and the most innovative automotive technologies are coming from Toyota and Honda, not Detroit, said analysts at the Center for Strategic and Budgetary Assessments in Washington.

Source: <http://www.military.com/news/article/car-makers-say-bailout-a-defense-issue.html?col=1186032310810>

8. *January 20, Register* – (National) **U.S., U.K. deploy manned unmanned aircraft to save bandwidth.** Bandwidth-starved military spyplane chiefs are resorting to the use of humans as airborne data-processing nodes, according to reports. Difficulties in deployment of unmanned robot surveillance craft have led to the purchase of basic civilian planes for use in intelligence work above Iraq and Afghanistan. For years now, ground commander's enemies in Southwest Asia have been begging for more Predator and Predator-B/Reaper Unmanned Air Vehicles (UAVs). The new plan, "Project Liberty," is to buy ordinary civilian twin-engine planes and fit them out with the lightweight sensors used by UAVs. Problems in delivering more video and groundscan radar imagery were seen as following from foot-dragging by the Air Force, demand outstripping supply, and failures by drone manufacturers to scale up their manufacturing base swiftly enough. It is now being suggested that the use of manned light aircraft as opposed to UAVs may be a matter of satellite bandwidth as much as UAV manufacturing and crewing issues. A Predator relaying full-motion hi-res video or detailed radar imagery is a massive bandwidth hog, and if it is out of line-of-sight from a friendly ground base it must normally use satcomms. Not only is this expensive, but there is a hard limit on how much satellite bandwidth is available in any given region even for the Pentagon.

Source: [http://www.theregister.co.uk/2008/11/20/manned\\_unmanned/](http://www.theregister.co.uk/2008/11/20/manned_unmanned/)

9. *November 20, Precision Castparts Corp.* – (Texas) **Equipment failure at Precision Castparts Corp.'s Wyman-Gordon forging facility.** This morning, the 29,000-ton forging press at Precision Castparts Corporation's (PCC) Wyman-Gordon (Wyman) facility in Houston, Texas, failed. This forge is used primarily to manufacture aircraft engine components. The company has a risk mitigation strategy in place in the event of such a failure. Wyman estimates that roughly 70 percent of the product handled on the 29,000-ton press can be moved with little interruption to another press in the Houston facility. The balance can be manufactured in other Wyman facilities within a reasonable period of time, an effort which will be coordinated with Wyman's customers. Wyman has begun an analysis of the extent of required repairs and expects to gain a better understanding of the situation within a week. "We have notified our customers about this unfortunate failure and will work closely with them to mitigate production interruptions," said the chairman and chief executive officer of PCC. "The primary output of the 29,000-ton press is aircraft engine components; the other Houston product lines are not affected."

Source: <http://www.marketwatch.com/news/story/Equipment-Failure-At-Precision-Castparts/story.aspx?guid={56E18206-F900-4E76-A9E2-1FE5B2C84FAE}>

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

## **Banking and Finance Sector**

10. *November 21, Philadelphia Inquirer* – (Pennsylvania) **Six charged with bilking settlement funds.** Six people, including two from the Philadelphia region, were charged Thursday with fraud in an alleged scheme to use dummy corporations, fake brokerage accounts, and virtual offices to steal \$41 million from settlement funds that were themselves set up to resolve earlier securities-fraud cases. An accountant with a firm that was paying out investor claims from those settlement funds was labeled the “eyes and ears” for the group, advising a coconspirator on when to submit fraudulent claims and on the availability of funds. The funds had about \$4.5 billion in assets. The acting U.S. Attorney said that the ring went to great lengths to make the claims seem legitimate. One member of the group, she said, even traveled to Singapore to mail documents to help make a fake company.

Source:

[http://www.philly.com/philly/business/20081121\\_Six\\_charged\\_with\\_bilking\\_settlement\\_funds.html](http://www.philly.com/philly/business/20081121_Six_charged_with_bilking_settlement_funds.html)

11. *November 21, Vicksburg Sun Herald* – (Mississippi) **Telephone scam targets bank information.** Authorities say Trustmark National Bank customers should beware of a telephone scam designed to obtain bank account information. The chief information security officer for the Jackson-based Trustmark said people should not give their information in response to an automated call. The scam consists of an automated message that tells customers their account has been compromised and their debit cards were deactivated as a safety precaution. Listeners are then given the option to reactivate their cards by entering their personal and account information.

Source: <http://www.sunherald.com/218/story/969452.html>

12. *November 20, Washington Post* – (International) **Web fraud 2.0: faking your Internet address.** One of the casualties from the unplugging of McColo Corp. is fraudcrew.com, a Web service that offered paying customers the ability to hide their identities online by routing their traffic through computers controlled by others. Fraudcrew, which has not been charged with any crime, offered subscribers a point-and-click way to mask the source of their Internet connections, so that Web sites could not tell the true location of visitors using the service. The site was advertised heavily on Russian online forums catering to computer hacking and identity theft. There are a number of services like those offered by Fraudcrew (Security Fix profiled another one earlier this year) that not only aid in hiding one’s identity online, but could also defeat security measures put in place by financial institutions. These masking services provide a software program that allows the user to pick from a drop down list of Internet addresses to proxy through. For example, if a user in Ukraine has stolen the user name and password that Joe from St. Louis uses to access his bank online, that user can simply select a node in the proxy list that is in St. Louis, and the bank site will be none the wiser that the person logging in is

not actually in St. Louis. “Although this type of technology isn’t new, it’s the first time I’ve seen it used like this for obviously criminal reasons,” said the director of security research and communications at McAfee AVERT Labs.

Source:

[http://voices.washingtonpost.com/securityfix/2008/11/web\\_fraud\\_20\\_faking\\_your\\_inter.html](http://voices.washingtonpost.com/securityfix/2008/11/web_fraud_20_faking_your_inter.html)

13. *November 20, Southampton Press* – (New York) **Quogue mayor’s investment firm also indicted on fraud charges.** Melhado, Flynn & Associates (MFA), the Manhattan-based investment firm headed by the Quogue Village mayor, has been indicted by the U.S. Attorney’s Office and charged with felony fraud and altering documents in an attempt to impede the subsequent investigation. The indictment comes several months after the mayor was indicted on the same charges. The indictment accuses the company and the mayor, who owns 9.3 percent of MFA and serves as its chief executive officer, of “cherry-picking” profitable accounts for the investment firm over a four-year period, and altering documents in an attempt to impede a subsequent investigation by the U.S. Securities and Exchange Commission. The mayor and MFA were each charged with one count of security fraud and one count of document alteration for illegally earning more than \$1.4 million for the investment company from November 2000 until June 2005, according to a copy of the indictment.

Source: [http://www.27east.com/story\\_detail.cfm?id=181701](http://www.27east.com/story_detail.cfm?id=181701)

14. *November 20, Expatica.com* – (International) **European police forces smash international bank card scam gang.** Authorities in Belgium, Ireland, Romania have smashed a Romanian crime gang which specialized in copying bank cards and operated worldwide, the Belgian prosecutor’s office said Thursday. The gang acting “on a global level” from their Belgian base, according to the Belgian authorities, is suspected of defrauding card users of millions of Euros. In Europe there were victims of their hi-tech “skimming” operations in Britain, Cyprus, Germany, Ireland, Italy, the Netherlands, Spain, Turkey and Romania itself. There were more suspected victims in Australia, Canada, the Dominican Republic, Morocco and New Zealand, the public prosecutor’s office said in a statement. A total of 34 police raids involving 250 officers were made in six EU nations — Belgium, Britain, Germany, Ireland, Romania and Spain. In those operations a total of 15 people were arrested.

Source: <http://www.expatica.com/be/articles/news/European-police-forces-smash-international-bank-card-scam-gang.html>

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

## **Transportation Sector**

15. *November 21, WKRC 12 Cincinnati* – (Ohio) **Hamilton man charged with local bomb threats.** The FBI arrested a Hamilton, Ohio, man for threatening to blow up several local landmarks. The man is accused of sending an e-mail detailing his plot to WKRC, a radio station, and FBI headquarters. The e-mail, sent November 13, used a fictitious name and claimed bombs would go off the next day on the Brent Spence Bridge, at Argosy Casino, Paul Brown Stadium, and the Cincinnati/Northern Kentucky

International Airport, among other targets. The Joint Terrorism Task Force arrested the man Thursday at a hotel. There was no sign the man actually possessed explosives.

Source: [http://www.local12.com/news/local/story.aspx?content\\_id=0fcb9aa8-da34-4de0-896c-fbacba395a52](http://www.local12.com/news/local/story.aspx?content_id=0fcb9aa8-da34-4de0-896c-fbacba395a52)

16. *November 20, Associated Press* – (California) **Calif. trains collide; no serious injuries.**

A Metrolink commuter train sideswiped a freight train November 20, causing no serious injuries but bringing back still-vivid memories of the deadly Chatsworth train wreck in the region just two months ago. The commuter train, carrying 15 passengers and crew, was heading east from downtown Los Angeles toward San Bernardino when it collided with a westbound BNSF train pulling onto a side track, authorities said. “Although this incident occurred at a low speed, any incident on the Metrolink system is unacceptable,” said the Metrolink Board Vice Chairman. “This incident will be fully investigated to determine the cause, and measures will be taken to ensure that incidents like this do not happen again.” It is unclear whether the Metrolink engineer in Thursday’s crash missed a signal. A Metrolink spokeswoman said the locomotive was staffed by an engineer and one other person, in accordance with new safety procedures instituted after the Chatsworth crash. Officials from the National Transportation Safety Board and the Federal Railroad Administration were investigating. Crews moved the two trains and reopened the tracks around 8 pm.

Source:

[http://hosted.ap.org/dynamic/stories/T/TRAINS\\_COLLIDE?SITE=NYONE&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/T/TRAINS_COLLIDE?SITE=NYONE&SECTION=HOME&TEMPLATE=DEFAULT)

17. *November 20, KCRA 3 Sacramento* – (California) **FBI seeks caller in plane bomb threat.** The Sacramento and Louisville, Kentucky, offices of the FBI said they are looking for information about a bomb threat that was called in Friday. Delta Flight 6081 left Milwaukee, Wis., and had already landed at the Greater Cincinnati International Airport when the call came in, the FBI said. The caller said there was a bomb on the plane. Investigators did not find any explosive devices on board. The FBI said officials tracked the call to a phone number that is associated with a truck stop in Ripon, California. Surveillance video shows a man using the phone near the time when the threat was made.

Source: <http://www.my58.com/news/18027944/detail.html>

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

## **Postal and Shipping Sector**

18. *November 21, News-Record* – (North Carolina) **Powder mailed from NJ won’t result in charges.** Deputies do not plan to pursue charges in connection with a mysterious powder that arrived at a woman’s home by mail Wednesday. The powder – ground chickpeas, according to the Guilford County Hazardous Materials Team – is not dangerous and did not come with any threat, according to the sheriff’s office. The powder came in an envelope without a return address but had a New Jersey postmark, said a detective.

Source: <http://www.news->

[record.com/content/2008/11/21/article/powder\\_mailed\\_from\\_nj\\_won\\_t\\_result\\_in\\_charges](http://record.com/content/2008/11/21/article/powder_mailed_from_nj_won_t_result_in_charges)

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

## **Agriculture and Food Sector**

19. *November 21, Pig Progress* – (International) **Russia: pork imports banned.** Russia has suspended imports of pork from Indiana Packers Corporation. The ban comes after reporting the discovery of salmonella in a pork shipment, according to USDA’s Food Safety and Inspection Service (FSIS). The Delphi, Indiana-based packer’s product will not be permitted into Russia effective November 24, FSIS has stated. According to reports, the USDA has not confirmed Russia’s reported finding of salmonella. “They have only reported these findings. We have no additional information,” said a FSIS spokeswoman.  
Source: [http://www.pigprogress.net/news/id1602-73720/russia\\_pork\\_imports\\_banned.html](http://www.pigprogress.net/news/id1602-73720/russia_pork_imports_banned.html)
20. *November 21, AgWeek* – (Delaware) **USDA designates Delaware as disaster area.** The state has formally been designated a natural disaster area because of the drought this summer June that damaged or killed many crops. USDA Farm Service Agency Executive Director Richard Bergold says Delaware farmers can receive low-interest emergency loan assistance. Loans can be used to pay production costs, essential expenses, and reorganization or refinancing costs.  
Source: [http://www.agweek.com/articles/?id=1598&article\\_id=12863&property\\_id=41](http://www.agweek.com/articles/?id=1598&article_id=12863&property_id=41)
21. *November 20, RedOrbit*– (International) **WHO calls for more research on foodborne illnesses.** The World Health Organization (WHO) reported Thursday that the number of foodborne diseases seem to be on the rise in both wealthy and poor nations. The director of food safety at the WHO said additional research is needed to assess how much illness and death is caused by contaminated food, such as tainted milk in China that sickened thousands and a U.S. outbreak of salmonella that sickened 1,400 people. During a meeting of experts, he said 30 percent of new infectious diseases come from bacteria, viruses, parasites, chemicals, and toxins introduced along food production chains. According to WHO figures, roughly 2.2 million children die each year from diarrheal illnesses, such as cholera, caused by contaminated water, food, and poor sanitation. And the director advises that food products be monitored at every stage of their handling. A Harvard Medical School professor explained that “Research into the long-term effects of foodborne disease is increasingly important because it is unquantified and goes on for decades.”  
Source: [http://www.redorbit.com/news/health/1601997/who\\_calls\\_for\\_more\\_research\\_on\\_foodborne\\_illnesses/](http://www.redorbit.com/news/health/1601997/who_calls_for_more_research_on_foodborne_illnesses/)

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

## Water Sector

22. *November 20, Daily Record* – (New Jersey) **100,000 told to boil water in aftermath of pipe break.** Water pressure is back to normal for most of the 100,000 customers in 18 towns affected by Tuesday's water-main break in Franklin Township, but the boil-water advisory for possible contaminants remains in effect for all the municipalities, said the external affairs manager for New Jersey American Water. Tap water intended for drinking or cooking should be boiled at a rolling boil for at least one minute, officials said. An American Water crew worked through the day yesterday to repair the 60-inch hole in the five-foot-wide, 50-year-old water main.  
Source: <http://www.dailyrecord.com/article/20081120/NEWS02/811200347/1123>
23. *November 20, Associated Press* – (Iowa) **Palo residents asked to limit sewer usage.** Palo residents are being asked to conserve their water and limit their use of sewer systems after the city's sewer treatment plant broke down. The man who oversees the eastern Iowa city's infrastructure, says officials are not sure what happened, but it appears that motors are burned out at the plant. He says the situation leaves the city a bit crippled. He says the city has alerted the state's Department of Natural Resources because some raw sewage may have to be released.  
Source: <http://www.chicagotribune.com/news/chi-ap-ia-palosewage.0,3067575.story>
24. *November 19, Star-Telegram* – (National) **Environmental group urges utilities to stop using chlorine gas.** Millions of people could be injured or killed by a chlorine leak at any of 10 water and sewer treatment plants in North Texas, according to an advocacy group that is pushing industries to use safer chemicals. Water officials in Fort Worth, Dallas, and Northeast Tarrant County said that they have reduced the amount of chlorine used at the plants, but that they cannot eliminate it entirely because it is vital to keeping the water free from disease. The Center for American Progress identified 303 industrial plants in the country where an accident or a terrorist attack could result in a catastrophic chemical leak. At the North Texas water plants, the report suggests using alternatives such as liquid bleach, ozone or ultraviolet light purification systems. Most of the water treatment plants have already switched to ozone purification systems, officials at all three water systems said. But they are required by the U.S. Environmental Protection Agency to maintain a small amount of chlorine in the water, known as a residual, to keep it disinfected until it reaches people's homes.  
Source: <http://www.star-telegram.com/804/story/1048536.html>  
See also: <http://deseretnews.com/article/1,5143,705264437,00.html>

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

## Public Health and Healthcare Sector

25. *November 21, HealthDay News* – (International) **New type of Ebola virus discovered.** A new species of the deadly Ebola virus has been identified by American and Ugandan scientists. The new virus, called Bundibugyo Ebola virus, caused an outbreak in western Uganda in 2007. It is genetically distinct from all other known Ebola virus species,

differing by more than 30 percent at the genetic level, said the scientists from the U.S. Centers for Disease Control and Prevention, Columbia University, the Uganda Virus Research Institute, and the Uganda Ministry of Health. Currently, there is no treatment or vaccine for Ebola infection in humans, which has a death rate of between 53 percent and 90 percent.

Source: <http://health.usnews.com/articles/health/healthday/2008/11/21/new-type-of-ebola-virus-discovered.html>

26. *November 21, Boston Globe* – (Massachusetts) **Boston launches flu shot tracking.** Using technology originally developed for mass disasters, Boston disease trackers are embarking on a novel experiment — one of the first in the country — aimed at eventually creating a citywide registry of everyone who has had a flu vaccination. The resulting vaccination map would allow swift intervention in neighborhoods left vulnerable to the fast-moving respiratory illness. The trial began Thursday afternoon, when several hundred people are expected to queue up for immunizations at the headquarters of the Boston Public Health Commission. Each received a bracelet printed with a unique identifier code. Information about the vaccine’s recipients, and the shot, will be entered into handheld devices similar to those used by delivery truck drivers. Infectious disease specialists in Boston and elsewhere predicted that the registry approach could prove even more useful if something more sinister strikes: a bioterrorism attack or the long-feared arrival of a global flu epidemic. In such crises, the registry could be used to track who received a special vaccine or antidote to a deadly germ.

Source:

[http://www.boston.com/news/local/massachusetts/articles/2008/11/21/boston\\_launches\\_flu\\_shot\\_tracking/](http://www.boston.com/news/local/massachusetts/articles/2008/11/21/boston_launches_flu_shot_tracking/)

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

## **Government Facilities Sector**

27. *November 21, Washington Post* – (Texas) **Verizon staff viewed Obama’s account.** Verizon Wireless said Thursday that a number of its employees have “accessed and viewed” the U.S. President-elect’s personal cellphone account without authorization. The company said all employees who accessed the account — whether they were authorized to or not — were immediately put on leave with pay. The firm said it was evaluating the circumstances of each employee’s access to the account to determine appropriate action, including disciplinary proceedings. The breach of personal data comes as some security experts question whether the U.S. President-elect, who used the Web as a central part of his campaign strategy, should for security purposes stop using devices to transfer e-mail and other data when he becomes President.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2008/11/20/AR2008112004198.html?hpid=topnews>

28. *November 21, Newsday* – (New York) **NYPD sergeant accused of accessing FBI terrorist list.** A New York Police Department sergeant has been charged with illegally accessing the FBI terrorist watch list. The sergeant surrendered yesterday and was awaiting an initial court appearance in federal court in Manhattan. He is accused of

accessing the information to aid an individual who was involved in a child custody dispute. The charge of accessing a computer without authorization carries a potential sentence of a year in prison.

Source: <http://www.newsday.com/news/local/newyork/ny-nyterr215936004nov21,0,4533629.story>

29. *November 20, WPEC 12 West Palm Beach* – (Florida) **Man makes bomb threats to postpone sentencing.** A 26-year-old called 911 and told dispatchers he put a bomb at the St. Lucie County Courthouse so he could postpone the November 7 sentencing for his felony case. The defendant called 911 twice that morning and said there was “C-4” in the building set to go off in 30 minutes, according to the St. Lucie County Sheriff’s Office. The building was evacuated at the time, and investigators were able to trace both calls back to the defendant through phone records.  
Source: <http://www.cbs12.com/sections/contactus/>

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

## **Emergency Services Sector**

30. *November 20, WSBT 22 South Bend* – (Indiana) **First responders concerned about safety at meth lab scenes.** First responders in Elkhart, Indiana, are trying to improve safety when they encounter drug scenes. Police are raiding an increasing number of meth labs and are working with firefighters to develop safety protocols. The labs are now turning up within the city limits at an increased rate. One of the most recent cases involved one found in an apartment unit last month. It caught on fire and exploded, injuring two people. Another was found in the upstairs of a vacant home in Elkhart. The increase has also caught the attention of the Elkhart Fire Department, which is training with the police department on safety measures.  
Source: <http://www.wsbt.com/news/local/34826379.html>
31. *November 20, Government Technology* – (National) **U.S. faces Al-Qaida terrorist threats, lacks vigilance since 9/11, speaker says.** The nation has become complacent since the September 11th attacks and lacks a healthy respect for the risks we face from terrorism, a 33-year veteran of law enforcement, who is also an attorney and internationally recognized source on risk management, said at the 56th International Association of Emergency Managers Conference November 18, 2008, in Kansas City, Kansas. He said that for a public safety agency or any other organization to be a “mission-ready organization” it has to be vigilant in terms of hiring good people, making them accountable, and continuously training. He suggested testing employees daily. He said when an employee signs on to a computer at the beginning of a shift, a drop-down box with a quick quiz would keep employees learning. He said employees should be tested regularly about their core critical roles before a disaster. “When a disaster occurs, most don’t know [their core roles] until after the fact,” he said.  
Source: <http://www.govtech.com/em/articles/563725>

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

## Information Technology

32. *November 21, ZDNet* – (International) **Mac OS X targeted by Trojan and backdoor tool.** Two pieces of malicious software affecting Apple’s Mac OS X appeared this week: a Trojan horse with the ability to download and install malicious code of an attacker’s choice, and a hacker tool for creating backdoors, according to security vendors. The Trojan — called ‘OSX.RSPlug.D’ by Intego, the Mac security specialist that discovered the threat — is a variant on an older piece of malicious code but with a new installer, Intego said. “It is a downloader, and it contacts a remote server to download the files it installs,” Intego said in an advisory. “This means that, in the future, the downloader may be able to install payloads [other] than the one it currently installs.” In other respects the Trojan is similar to previous versions of RSPlug, which first surfaced in October 2007, Intego said. It installs a piece of malicious code known as DNSChanger, which routes the user’s internet traffic through a malicious DNS server, leading users to phishing websites or pages displaying advertisements. Intego said OSX.RSPlug.D has been widely confused with a separate threat publicised this week by several security firms. That threat is called OSX.TrojanKit.Malez by Intego and OSX.Lamzev.A by other vendors, including Symantec and Trend Micro. Security vendors have long warned that the Mac platform is not as secure as some users might like to believe. Apple had not responded to a request for comment at the time of publication  
Source: <http://news.zdnet.co.uk/security/0,1000000189,39559174,00.htm>
33. *November 20, IDG News* – (International) **Researchers find vulnerability in Windows Vista.** An Austrian security vendor has found a vulnerability in Windows Vista that it says could possibly allow an attacker to run unauthorized code on a PC. The problem is rooted in the Device IO Control, which handles internal device communication. Researchers at Phion have found two different ways to cause a buffer overflow that could corrupt the memory of the operating system’s kernel. In one of the scenarios, a person would already have to have administrative rights to the PC. In general, vulnerabilities that require that level of access somewhat undermine the risk since the attacker already has permission to use to the PC. But it may be possible to trigger the buffer overflow without administrative rights, said Phion’s director of endpoint security software. The vulnerability could allow a hacker to install a rootkit, a small piece of malicious software that is very difficult to detect and remove from a computer, the director said. Phion notified Microsoft about the problem on October 22. Microsoft indicated to Phion that it would issue a patch with Vista’s next service pack. Microsoft released a beta version of Vista’s second service pack to testers last month. Vista’s Service Pack 2 is due for release by June 2009.  
Source: <http://www.itworld.com/windows/58144/researchers-find-vulnerability-windows-vista>
34. *November 19, Dark Reading* – (International) **Broadband explosion in China and India to fuel bots, spam.** Botnet operators have begun to quietly expand their recruiting efforts to China and India, as broadband adoption begins to take off in these countries. China and India will reach a nearly 30 percent rate of broadband adoption to the home during the next one to two years, providing botnet operators access to more potential bot

victims, chief security analyst for MessageLabs says. “That will have implications that the whole world will feel,” he says, like when the broadband wave hit the United States and Europe around 2003. “The Sobig virus [here] in January of 2003 was no coincidence. It was about exploiting broadband,” he says.

Source:

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=212100876>

## Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@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

35. *November 21, WSB 750 Atlanta* – (Georgia) **State outsources IT work.** The State of Georgia has decided to contract out its Information Technology operations. The governor announced AT&T and IBM were the sole bidders on two separate contracts worth \$346 million and \$873 million respectively. “Providing technology services is not a core competency of state government...we’ve tried and its not one of the things that we do best,” he says. He cites crashing servers as well as leaky roofs and rodents in the office building that houses the state’s primary data system. “I was frightened because I could not guarantee Georgia citizens that their data was secure or that we were spending our IT dollars in the best way possible,” he says.

Source: <http://wsbradio.com/localnews/2008/11/state-outsources-it-work.html>

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

## Commercial Facilities Sector

36. *November 21, Associated Press* – (Indiana; Ohio) **Man arrested in Bengals’ stadium bomb threat.** FBI officials said Friday they arrested a man who allegedly threatened to blow up the Cincinnati Bengals’ stadium and other area landmarks. The 42 year old man is accused of sending e-mails to two local media outlets and to the FBI threatening Paul Brown Stadium, four bridges over the Ohio River, the Cincinnati/Northern Kentucky International Airport, and an Indiana casino, a FBI spokesman said. The man was arrested Thursday at a hotel in Erlanger, Kentucky, and was being held on federal charges of making bomb threats and distributing a bomb hoax. The man’s father said his son has mental issues and is on medication and he said he doesn’t believe his son really planned to carry out any threats.

Source: <http://www.msnbc.msn.com/id/27841930/>

37. *November 20, Denver Post* – (Colorado) **Gas leak blamed in fatal Pueblo explosion.**

The thunderous explosion at Pueblo's historic Branch Inn that killed one person and seriously injured several others was caused by natural gas that migrated into the restaurant's basement from a leaking gas line, local and federal officials said today. A spokesman for the Pueblo Fire Department, said the leak occurred in a feeder line under Pueblo's C Street. The gas migrated through the soil to the basement of the Branch Inn, the spokesman said. There it accumulated and was ignited by one of numerous possible sources, said a spokesman for the Bureau of Alcohol, Tobacco, Firearms and Explosives. Those included a compressor for a freezer, other electrical appliances and candles. A plastic sleeve had been inserted into the older iron pipe of the feeder line. Where it connected with the main gas line under the street may have been where the problem or leak occurred. Natural gas can normally be detected because of the "rotten egg" smell that is added to it to alert people to a leak. But officials said the distinctly pungent odor was filtered out by the soil. Just how long there had been a leak is still under investigation, said officials. Officials said the cause of the blast has been officially classified as "accidental."

Source: [http://www.denverpost.com/popular/ci\\_11032653](http://www.denverpost.com/popular/ci_11032653)

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

## **National Monuments & Icons Sector**

38. *November 20, Associated Press* – (Pennsylvania) **Environmentalists sue over Pa. forest drilling.** Environmental groups and U.S. Forest Service employees are suing the Forest Service over its approval of several oil and gas drilling projects in the Allegheny National Forest that they claim will harm wildlife and the environment. The suit says the agency approved the plans without the necessary environmental review. The suit was filed Thursday in federal court. The Allegheny Defense Project says gas and oil drilling has increased dramatically in the forest. The group says drilling and numerous roads built to support it can destroy wildlife habitat and hurt recreation opportunities. The Forest Service says it has not seen the suit and cannot comment. The employees are members of the Forest Service Employees for Environmental Ethics.

Source: [http://www.ldnews.com/news/ci\\_11033124](http://www.ldnews.com/news/ci_11033124)

39. *November 19, Associated Press* – (Georgia) **Blairsville man convicted of marijuana farming.** A North Georgia man has been convicted of conspiracy to grow hundreds of marijuana plants in and around the Chattahoochee National Forest. A federal jury in Gainesville found Andrew N. Cox, 45, of Blairsville guilty Wednesday. Authorities say Cox fled after his indictment and was a fugitive for three years before his February 13 arrest in Casa Grande, Arizona. Cox and three others were accused of planting and cultivating marijuana in 2004, using a landscaping business as a front. Co-conspirators Jose Quezadas-Fierros, Paciano Vargas-Hernandez, and Mayolo Vargas-Villeneuve pleaded guilty in 2004 and 2006. With two prior felony drug convictions and at least 1,000 marijuana plants involved, Cox faces life in prison.

Source:

[http://www.ajc.com/news/content/metro/stories/2008/11/19/blairsville\\_marijuana\\_farm.html](http://www.ajc.com/news/content/metro/stories/2008/11/19/blairsville_marijuana_farm.html)

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

## **Dams Sector**

40. *November 20, Howard County Times* – (Maryland) **State to remove dams for spawning fish.** About 15 years ago, Maryland spent more than \$3 million to make it easier for spawning fish to swim upriver past three aging dams along the Patapsco River. The structures they built – known as “fish ladders” – were part of a statewide effort to bring once-prolific shad and herring back to the rivers that feed the Chesapeake Bay. Now, however, state officials say the ladders did not work as well as they hoped and that they are seeking to remove the dams instead, a solution they considered 15 years ago, but rejected as too costly. The dams, many of which were built in the early 1900s to serve now-defunct mills, have blocked those spawning runs, leading, throughout the 20th century, to precipitous declines in the number of shad and herring that were being caught in Maryland. Destroying the dams is the best way to clear the way for spawning fish, said a program manager in the fisheries department of the Department of Natural Resources. Removing the dams would cost about \$5 million, officials say.  
Source: <http://www.explorehoward.com/news/13278/state-remove-dams-spawning-fish/>
  
41. *November 20, Daily Herald* – (Illinois) **Des Plaines dedicates home-saving Levee 50.** Des Plaines held a ribbon-cutting ceremony Thursday to celebrate the completion of the Levee 50 flood control project. “It took seven years to get this done, but the flooding we had back in September proved that this levee works,” said the mayor. “We had no flooding east of the levee and that is what this was meant to prevent.” The combination of the levee wall and new pumps was credited at the time with holding back enough water to spare about 400 homes and businesses in Des Plaines from taking in water. The project cost about \$15 million, of which the city of Des Plaines contributed about \$1.3 million. Levee 50 is just one of six federal projects in this watershed area that are planned to control flood waters at an estimated cost of about \$72 million. The plan for those projects grew out of severe flooding in 1986 and 1987.  
Source: <http://www.dailyherald.com/story/?id=252323&src=1>

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

## **DHS Daily Open Source Infrastructure Report Contact Information**

**DHS Daily Open Source Infrastructure 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>

## **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions: Send mail to [NICCReports@dhs.gov](mailto: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 [NICCReports@dhs.gov](mailto:NICCReports@dhs.gov) or contact the DHS Daily Report Team at (202) 312-3421 for more information.

---

## **Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.