



## Department of Homeland Security Daily Open Source Infrastructure Report for 19 May 2008

Current Nationwide Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF TERRORIST ATTACKS

[For info click here](#)

- According to Newsday, National Guard troops that have stood guard at four upstate New York nuclear power plants since shortly after the September 11, 2001, terrorist attacks are being withdrawn this summer. (See item [10](#))
- The Associated Press reports investigators have concluded that two military helicopters were vandalized on the production line at a Boeing factory near Philadelphia, the U.S. Defense Department said Thursday as it offered a reward in the case. (See item [11](#))

### 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. *May 16, Bloomberg* – (International) **Oil rises to record above \$127 on Goldman Report, China demand.** Crude oil rose above \$127 a barrel for the first time, after Goldman Sachs Group Inc. raised its forecast and on speculation Chinese diesel purchases will strain supplies. Goldman boosted its price estimate for the second half of this year to \$141 a barrel, from \$107, citing supply constraints. China may increase fuel imports to generate power after the most powerful earthquake in 58 years killed more than 22,000 and damaged hydroelectric plants. Crude oil for June delivery rose \$2.89, or 2.3 percent, to \$127.01 a barrel at 11:16 a.m. on the New York Mercantile Exchange. The contract climbed to \$127.82 Friday.

Source:

<http://www.bloomberg.com/apps/news?pid=20601072&sid=a5ouK4bXBdaA&refer=energy>

2. *May 16, Hess Corporation* – (National) **MMS planning for hurricanes.** The Minerals Management Service (MMS) has announced that preparations for the 2008 hurricane season are now underway. A number of actions to take have been discussed at a meeting, the MMS says, noting that key preparations will be to improve energy security for the nation while also offering environmental protection and safety for personnel working in the Gulf of Mexico. The deputy director of the MMS said that through working with all affected parties, including the American Petroleum Institute, the Coast Guard, and the oil and gas industry, the organization is in a good place to ensure that oil and gas production from the region is disrupted as little as possible during the hurricane season.

Source: <http://www.hessenergy.com/common/NewsItem.aspx?ArticleId=18597044>

3. *May 15, KBAK 29 Bakersfield* – (California) **Refinery still not responding to questions about contaminated gas.** More than a week after contaminated gasoline is discovered in Kern County, the refinery responsible for the problem still will not answer questions about what happened. The contaminated gas has been tracked back to the Kern Oil and Refining Company. Eyewitness News first uncovered this consumer alert on May 7 and was first alerted to the problem when viewers reported their cars had been damaged by bad gas. A local says the company told her the gas had sediment in it, and they were still trying to track down exactly what that was. Kern County's Department of Agriculture and Measurement Standards said it is their understanding there was some kind of filter-system failure at the refinery that affected one batch of gas. The department now reports they have received about 150 complaints about the contaminated gas, and 50 of the cases seem to be related to the gas from Kern Oil. The department says the contaminated gas ended up at 24 gas stations and one car dealership in Kern County. Some of that gas was also delivered to stations in seven other counties.

Source: <http://www.eyeforyou.com/home/18992184.html>

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

## **Chemical Industry Sector**

Nothing to Report

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

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

4. *May 16, New York Times* – (International) **Western experts monitor China's nuclear sites for signs of earthquake damage.** China's main centers for designing, making, and storing nuclear arms lie in the shattered earthquake zone, leading Western experts to look for signs of any damage that might allow radioactivity to escape. A senior federal official said the U.S. was using spy satellites and other means to try to monitor the

sprawling nuclear plants. “There appear to be no immediate concerns,” the official said. A former director of intelligence at Los Alamos National Laboratory and an expert on the Chinese nuclear program said he had immense regard for Chinese weapons scientists and assumed that many of their nuclear plants had been built to ride out the pounding of an earthquake or other disasters, natural, or man-made.

Source: <http://mobile.nytimes.com/article?a=165665&f=20&p=0>

5. *May 16, Boston Herald* – (Massachusetts) **Plymouth nuke, union reach 11th-hour pact.** A strike has been averted at Plymouth’s Pilgrim Nuclear Power Station. The plant’s owner, Entergy, and the Utility Workers of America’s Local 369 reached a contract agreement for 254 workers Thursday night. In a press release, Entergy said the “nonstop negotiations to prevent a strike were successful,” with the terms of the new contract lasting four years.  
Source: <http://www.bostonherald.com/business/general/view.bg?articleid=1094404>
6. *May 16, Rutland Herald* – (Vermont) **Yankee cited for security violations.** The owners of Vermont Yankee nuclear plant have been cited for security violations by the U.S. Nuclear Regulatory Commission (NRC). A spokesman for the NRC said the violation was serious enough to warrant increased inspections of Entergy Nuclear’s security at the Vernon reactor. The security breach was termed “an escalated enforcement action,” in a letter sent to the Entergy Nuclear site vice president. The NRC spokesman said the security violation occurred in February, and he would only say that it did not involve “an inattentive security officer.” He said Entergy Nuclear had reported the violation to the NRC. “We agreed with the NRC and did not contest,” said an Entergy Nuclear spokesman. He said Wackenhut Nuclear Services still provided security services at Vermont Yankee.  
Source:  
<http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20080516/NEWS04/805160347/1003/NEWS02>
7. *May 16, York Daily Record* – (Pennsylvania) **TMI plant will have additional oversight measures.** The U.S Nuclear Regulatory Commission (NRC) will boost its number of inspections at Three Mile Island Unit 1 based on a security-related violation that occurred at the plant last summer. The violation did not jeopardize public health and safety. “The underlying issue was identified by the company, and the NRC has verified that appropriate actions have been taken to address the problem,” said a spokesman for the NRC. Commission officials would not comment on the details of the finding, billed as “greater than very low safety significance,” but they did say the violation did not involve inattentive guards.  
Source: [http://ydr.inyork.com/ci\\_9276198](http://ydr.inyork.com/ci_9276198)
8. *May 16, Knoxville News Sentinel* – (Tennessee) **Drug testing grows under DOE program.** A new U.S. Department of Energy (DOE) program will make thousands of Oak Ridge workers potentially subject to random drug testing. As part of DOE’s Drug-Free Federal Work Place Program, Oak Ridge employees with “Q” or “L” security clearances will be included in a pool of workers randomly tested at a rate of 30 percent

annually. The pool available for random testing at ORNL will include about 1,800 workers with security clearances. The Y-12 National Security Complex already conducts random testing for about 2,500 employees who work in the most sensitive positions at the plant. That program, called the Human Reliability Program, includes both drug and alcohol testing. The new order will expand the drug testing to include another 4,500 workers – contractor and federal employees – at the Oak Ridge site, according to a government spokesman at Y-12. A spokesman for ORNL said Thursday that the drug testing would not begin for at least a couple of months because of the 60-day notice required.

Source: <http://www.knoxnews.com/news/2008/may/16/drug-testing-grows-under-doe-program/>

9. *May 16, Associated Press* – (Washington) **Tours of Hanford nuclear waste site draw interest.** The Hanford nuclear reservation will draw some 2,000 tourists this year. Tourists are not allowed close enough to the cleanup operations to be in danger from Hanford's contaminants, largely found in the soil and water. From a distance, visitors watch workers in white protective suits bury mercury-contaminated soil in a landfill. They gawk at massive cranes brought in to build a plant that will encase radioactive waste in glass. The B Reactor is the showpiece of the tours, which also highlight the remnants of World War II and Cold War weapons production. The U.S. Department of Energy posts tour dates for the site on its Web site each spring. Visitors preregister online, and the bus tours fill up within minutes. Only U.S. citizens are permitted.

Source:

<http://ap.google.com/article/ALeqM5idATeIm5ZlqP4RSY2dzCGzTWOAKQD90MN3R80>

10. *May 15, Newsday* – (New York) **National Guard troops pulled from nuclear plants.** National Guard troops that have stood guard at four upstate New York nuclear power plants since shortly after the September 11, 2001, terrorist attacks are being withdrawn this summer. A spokesman for the state Division of Military and Naval Affairs tells WSTM-TV in Syracuse that there was not any money included in the state budget for keeping the troops at nuclear plants near Oswego and Ginna. A spokeswoman for Constellation Energy, which operates the two nuclear plants at Nine Mile Point in Scriba, says it was notified that the troops will be withdrawn from there this summer. The Division of Military and Naval Affairs says about 100 troops are stationed at the four plants, and deployments at others in the state are under review.

Source: <http://www.newsday.com/news/local/wire/newyork/ny-bc-ny--nuclearplantsecur0515may15,0,4494612.story>

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

## **Defense Industrial Base Sector**

11. *May 15, Associated Press* – (National) **Two Army helicopters at Pa. plant vandalized.** Investigators have concluded that two military helicopters were vandalized on the production line at a Boeing factory near Philadelphia, the U.S. Defense Department said Thursday as it offered a reward in the case. Federal officials were handing out fliers to

workers at the Boeing Rotorcraft Systems plant listing a \$5,000 reward in the damaging of the two H-47 Chinook helicopters. “We have determined that this was a deliberate act and not an accident,” said the resident agent in charge of the Philadelphia area office of the Defense Criminal Investigative Service. A production line at the plant has not been fully functional since Tuesday, when two workers found what the company called irregularities in the helicopters. A U.S. congressman has said he was told that wires that appeared to be broken or severed were found in one helicopter and that a suspicious washer was found in a second.

Source: <http://www.msnbc.msn.com/id/24652807/>

12. *May 15, Web Wire* – (National) **New Orleans businessman pleads guilty to espionage charge involving China.** A New Orleans man pleaded guilty Tuesday in Virginia to a one-count criminal information charge for conspiracy to deliver national defense information to a foreign government, namely, the People’s Republic of China. He was arrested in February 2008 on a criminal complaint charging this same offense. According to a statement of facts filed with the man’s plea agreement, the criminal conduct spanned the time period of March 2007 to February 2008. During this time, the man, a naturalized U.S. citizen, obtained national defense information from a weapons systems policy analyst at the Defense Security Cooperation Agency. The information pertained primarily to U.S. military sales to Taiwan and U.S. military communications security and was classified at the Secret level. In March 2008, the analyst pleaded guilty to conspiracy to deliver national defense information to a person not entitled to receive it. Espionage charges are still pending against an alleged conspirator.

Source: <http://www.webwire.com/ViewPressRel.asp?aId=65636>

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

## **Banking and Finance Sector**

13. *May 16, Buffalo News* – (New York) **Amherst investment firm linked to fraud.** Attorneys for the federal government took emergency legal action Thursday to halt what they called a multimillion dollar fraud scheme involving an Amherst investment company located in Buffalo, New York. Officials of Watermark Financial Services and some associated companies are accused in a non-criminal complaint of bilking approximately 90 investors, many of them senior citizens. The U.S. Securities and Exchange Commission filed court papers asking a district judge to issue a temporary restraining order to stop the investment venture and freeze the company’s assets.
- Source: <http://www.buffalonews.com/145/story/348085.html>
14. *May 15, Consumer Affairs* – (National) **Maryland shuts down investment scam.** Investment fraud continues to plague unwary consumers, particularly seniors. Scam artists can exploit this trust unless consumers carefully assess an investment. Maryland authorities have completed their prosecution of an investment “advisor” they say took more than \$2 million from 21 investors and spent it on himself. The former operator of Forrester Financial Group in Phoenix pled guilty in Baltimore to felony theft and fraudulent securities practices. A Maryland Attorney General says the state’s investigation revealed that from January 2003 to March 2007, while acting as a

securities broker-dealer agent, the suspect took \$2,219,975 from investors with the express representation that he would place their money in a high interest, short term investment opportunity that he referred to as the “Private Funding Group.” Fraud investigators say investors should never trust their finances to anyone promising high returns with little or no risk, and should always seek counsel from family or trusted friends before investing.

Source: [http://www.consumeraffairs.com/news04/2008/05/md\\_investment\\_scam.html](http://www.consumeraffairs.com/news04/2008/05/md_investment_scam.html)

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

## **Transportation Sector**

15. *May 16, Reuters* – (National) **FAA studying American’s lightning checks procedure: report.** Federal aviation officials are examining why AMR Corp’s American Airlines asked mechanics to start skipping some safety checks to detect damage to planes from suspected lightning strikes, the Wall Street Journal said on Friday, citing internal company and agency documents. The regional Federal Aviation Administration (FAA) office overseeing the airline is asking questions about the issue, in the first step of a possible formal investigation, the report said, citing people familiar with the details. If the FAA concludes that American exceeded its authority in making the changes, it could face formal enforcement proceedings resulting in a civil fine and another change in procedures, the Journal added.

Source:

<http://uk.reuters.com/article/rbssIndustryMaterialsUtilitiesNews/idUKN1616778420080516>

16. *May 16, Aero-News* – (Florida) **FAA says pilots using TMB should watch for gunfire.** WPLG-10 reports the Federal Aviation Administration (FAA) recently took the unusual step of issuing a Notice to Airmen for pilots flying into Kendall/Tamiami Executive Airport southwest of Miami, Florida, after bullet holes were found in the fuselages of two aircraft based at the busy general aviation field. To avoid the chances of being hit by gunfire, pilots are advised to make steep approaches into the airport, and to make haste when climbing out on takeoff. The bullet holes were found over a two-month period, notes CBS affiliate WFOR-4. The FAA issued the request following an investigation by the Miami-Dade police department. At this point, it is not known whether the gunfire was the byproduct of another criminal activity, or a random event.

Source: <http://www.aero-news.net/index.cfm?ContentBlockID=683b4373-3357-44e9-be65-96bd3146ccba>

17. *May 15, Associated Press* – (North Dakota) **Flight attendant accused of setting fire on airplane.** A flight attendant angry about his work route set a fire in an airplane bathroom, forcing an emergency landing, authorities said. The Compass Airlines flight carrying 72 passengers and four crew members landed safely in Fargo, North Dakota, on May 7 after smoke filled the back. No injuries were reported. The plane was flying from Minneapolis to Regina, Saskatchewan, authorities said.

Source: <http://www.abcnews.go.com/US/wireStory?id=4866671>

18. *May 15, Associated Press* – (Colorado) **Federal agents trigger security breach at Denver airport.** Federal agents pursuing two suspects triggered a security breach Thursday at Denver International Airport, shutting down passenger screening for about 20 minutes. Two Immigration and Customs Enforcement agents and a Secret Service agent dressed in plain clothes went through the passenger screening area without being verified by screeners. The Transportation Security Administration closed down screening stations and stopped the airport's trains while federal air marshals and police searched for the agents. They were found on Concourse B and had arrested the suspects. Security lines were back to their normal length within an hour, an airport spokesman said.  
Source: [http://www.examiner.com/a-1393933~Federal\\_agents\\_trigger\\_security\\_breach\\_at\\_Denver\\_airport.html](http://www.examiner.com/a-1393933~Federal_agents_trigger_security_breach_at_Denver_airport.html)
19. *May 15, Post-Standard* – (New York) **Man stopped from boarding plane with knife.** A man with a knife while trying to board a Boston-bound airliner at Syracuse Hancock International Airport, New York, was detained before the knife was taken and he was allowed to go, Syracuse police said. The passenger had a four-inch lock-blade knife under his shirt, police said. The suspect told police he is a member of the Sikh religion and he carries the knife as part of his religion, police said. He had forgotten he had the knife on him, he told police.  
Source:  
[http://www.syracuse.com/news/index.ssf/2008/05/man\\_stopped\\_from\\_boarding\\_plane.html](http://www.syracuse.com/news/index.ssf/2008/05/man_stopped_from_boarding_plane.html)
20. *May 15, Canadian Press* – (International) **Passport theft in Canada increasing dramatically.** After a dramatic spike in reports of lost and stolen passports over the past two years, Passport Canada is giving additional scrutiny to passport applications across the country and warning travelers to protect their travel documents. In 2007, 37,650 passports were reported lost or stolen, compared to 24,792 in 2005. The numbers, obtained by the Canadian Press, were recently circulated in a memo warning staff to double-check applications for new passports when the old document is reported missing. "Lost and stolen passports are extremely valuable to criminal organizations to facilitate and perpetrate illegal/clandestine operations such as human trafficking, smuggling, money laundering and terrorism," said the memo. But security experts warned Wednesday that increased security features and better communication between government departments may not be enough to stay ahead of organized criminal groups, who make big money on stolen passports.  
Source:  
[http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20080515/passport\\_theft\\_080515/20080515](http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20080515/passport_theft_080515/20080515)

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

## **Postal and Shipping Sector**

Nothing to Report

## **Agriculture and Food Sector**

21. *May 16, Delta Farm Press* – (National) **Discovery of cattle disease ‘wakeup call.’** The discovery of malignant catarrhal fever in cattle should not be a reason for panic but is a “wakeup call” for better animal identification, according to an LSU AgCenter veterinarian. The National Veterinary Services Laboratories in Ames, Iowa, recently reported that three cases of the wildebeest strain of the disease were confirmed in cattle originating from Texas. “The cattle in Texas were exposed to captive wildebeests at the same ranch,” the veterinarian said. “Then the 134 animals subsequently were sold and later traced to ranches in Alabama, Arkansas, Georgia, Illinois, Louisiana, and Mississippi,” she added. “One heifer exposed to the wildebeests that was shipped to Louisiana has since died of the disease.” She said the cases of malignant catarrhal fever are much less significant than other diseases, but she said they do serve as warnings about what needs to be done. She said this incident also serves as a warning about the dangers of mingling domestic and exotic hooved animals. “Producers should have very strict biosecurity plans in place to prevent spread of contagious diseases between groups of animals,” she said. “This includes quarantining newly purchased cattle or cattle returning to the farm. Malignant catarrhal fever is caused by a herpes virus. “Wildebeests and sheep are carriers of the virus and do not display signs of the disease,” she explained. “But they can transmit the disease to cattle – in which it is highly fatal. “The good news is that transfer of this disease from cattle to cattle is very rare, so continued spread is very unlikely. It also is not a threat to human health or the food supply.” The sheep strain of malignant catarrhal fever occurs naturally in the U.S., but the wildebeest strain is foreign to the U.S.

Source: <http://deltafarmpress.com/news/cattle-disease-0516/>

22. *May 16, Reuters* – (International) **Bluetongue animal vaccination starts in most of EU.** EU farmers have mostly started vaccinating animals against bluetongue, the virus that ravaged northern Europe’s cattle and sheep in 2007, but success depends on vaccine supply and speed of applying it, officials say. Bluetongue swept across 11 EU countries last year and struck again recently in parts of Italy and France. Spread by midges, the virus had previously tended to occur in more southerly EU regions until 2006, when it moved further north. Bluetongue does not affect humans and there is no risk of contracting it by consuming milk or meat from affected animals. Vaccination plans have now begun in most countries where animals have been affected, officials say. The disease comes in different strains: in more southerly countries serotype 1 has been prevalent; while in northerly areas serotype 8 – for which a vaccine has only recently become available – has dominated. But there is some crossover, especially in France, and this has worried many experts. “There are problems in France with serotype 1,” said one official at a national farmers’ organization. “But those areas are crossing and they don’t have much vaccine. Britain is about the only country with enough vaccine.” The bluetongue virus is characterized by inflammation of the mucous membranes, congestion, swelling, and hemorrhages. Sheep are often the worst affected animals.

Source:

<http://www.reuters.com/article/scienceNews/idUSL1688914920080516?pageNumber=1>

## **Water Sector**

23. *May 16, South Florida Sun-Sentinel* – (Florida) **Water district halts work on Everglades reservoir due to lawsuit.** A legal showdown over how to restore water flows to the Everglades could stop construction on a massive reservoir rising in western Palm Beach County, Florida. The South Florida Water Management District Governing Board voted Thursday to suspend construction of the 16,700-acre reservoir as of June 1, blaming a year-old legal challenge filed by the Natural Resources Defense Council. The district will pay its contractor up to \$11.4 million while work is stopped. The defense council sued to ensure that water in the reservoir gets directed to the Everglades and not siphoned off for agriculture or drinking water.  
Source: <http://www.sun-sentinel.com/news/local/southflorida/sfl-515gladesreservoir,0,7892451.story>
24. *May 15, Tampa Tribune* – (Florida) **2 more contaminated wells discovered.** Two more private irrigation wells in the Azalea neighborhood of St. Petersburg have turned up contaminated with industrial waste, bringing the number to eight residential wells tainted by the nearby Raytheon plant, the latest test results show. Department of Environmental Protection (DEP) is sending notices to the two homeowners informing them their groundwater is polluted with industrial chemicals. In addition, three test wells in residential areas near the Raytheon plant tested positive recently for contaminants. What is more, earlier test wells revealed contamination under parks, playgrounds, and homes within a half-mile radius of the Raytheon plant. Those wells are not used for irrigation. DEP officials have said they are not sure whether the contaminated wells pose any danger to homeowners or their pets. Raytheon has said that a health risk assessment report in 2005 indicates there is no threat to public health. The pollutants include such industrial chemicals as 1,4-Dioxane, TCE, and vinyl chloride, all considered hazardous to humans. The DEP expects to receive a final assessment report from Raytheon on the extent of groundwater pollution by May 30. A cleanup plan is due 60 days after that.  
Source: <http://suncoastpinellas.tbo.com/content/2008/may/15/2-more-contaminated-wells-discovered/?news>
25. *May 15, WDBJ 7 Roanoke* – (Virginia) **Water contaminated in Chatham.** Something is polluting the water in Chatham, Virginia. A large amount of debris and organic matter washed in during last week's storms. The water plant was shut down Monday to clean it all out. But town officials say they are still seeing unsafe levels of contamination. Town officials believe it may be coming from fertilizers, but they have asked Virginia's Department of Environmental Quality to figure out what is polluting the water.  
Source: [http://www.wdbj7.com/Global/story.asp?S=8331155&nav=menu368\\_21\\_8\\_2](http://www.wdbj7.com/Global/story.asp?S=8331155&nav=menu368_21_8_2)

## Public Health and Healthcare Sector

26. *May 16, Fox News* – (National) **Salmonella outbreak linked to dry dog food.** An outbreak of Salmonella has been linked to contaminated dry dog food for the first time ever, said officials from the Centers for Disease Control and Prevention. CDC officials said dry dog food may be an under-recognized source of illness in humans, and they are unsure how the bacteria got into the dog food. Usually, Salmonella comes from undercooked meats and eggs. Humans became infected with Salmonella in 2006 and 2007 from dry dog food produced by Mars Petcare in Pennsylvania. Dogs were not affected, according to the May 16 issue of the CDC's Morbidity and Mortality Weekly Report, but a number of those affected were infants.  
Source: <http://www.foxnews.com/story/0,2933,356203,00.html>
27. *May 16, Press Association* – (International) **Cyclone survivors face disease risk.** Lack of clean water will be the biggest killer in cyclone-hit Myanmar in the coming days, the international Red Cross warned. Hundreds of thousands of victims risk falling victim to diseases such as dysentery, the head of operations for the International Federation of Red Cross and Red Crescent Societies said. "If clean water isn't available it's going to be the biggest killer in the post-disaster environment," said an official.  
Source: [http://ukpress.google.com/article/ALeqM5gD\\_5n2vEOyHuEfEjrredV2R5-Vw](http://ukpress.google.com/article/ALeqM5gD_5n2vEOyHuEfEjrredV2R5-Vw)
28. *May 15, TMCnet* – (National) **Hospital will use wireless technology.** Virginia Commonwealth University Health System (VCUHS) will deploy Horizon, a Converged Wireless Solution of InnerWireles, in its new 385,000-square-foot Critical Care Hospital to ensure better wireless connectivity for mission- and life-critical applications. VCUHS, by using Horizon, can optimize its wireless ecosystem, which includes 802.11, wireless telemetry, cellular phones and PDAs, clinical carts, laptops, tablet PCs, pagers, and two-way radios. "Because the acuity of our patients is so high, it's imperative that our wireless infrastructure work at all times so clinicians can receive alerts, notifications and information about their patients in real-time via the numerous wireless devices that we will have in place," said the VP and CIO of VCUHS.  
Source: <http://hdvoice.tmcnet.com/topics/unified-communications/articles/28159-hospital-will-use-wireless-technology.htm>

---

## Government Facilities Sector

29. *May 16, Bridgeton News* – (New Jersey) **Courthouse bomb threat.** A bomb scare Thursday morning forced an evacuation of the Cumberland County Courthouse in Bridgeton, New Jersey. Although no explosive device was found, the threat resulted in activities at the courthouse being put on hold for 12 hours while the county sheriff's department searched the building. The bomb threat was called into the county 911 center at about 10:38 a.m., according to the county sheriff's department. The caller said there was a bomb at the courthouse with a 20-minute detonation time. Thursday's bomb threat was the most recent in a series of bomb threats against the county courthouse in the last

several months, all of which have been unfounded. No one has been arrested in connection with the bomb threats.

Source: <http://www.nj.com/news/bridgeton/local/index.ssf?/base/news-14/121091822251960.xml&coll=10>

30. *May 15, IDG News Service* – (National) **DNS trouble knocks NSA off Internet.** A server problem at the U.S. National Security Agency has knocked the secretive intelligence agency off the Internet. The agency's Web site was unresponsive at 7 a.m. Pacific time Thursday and continued to be unavailable throughout the morning for Internet users. The Web site was unreachable because of a problem with the NSA's DNS servers, said the chief research officer with Arbor Networks. DNS servers are used to translate things like the Web addresses typed into machine-readable IP addresses that computers use to find each other on the Internet. The agency's two authoritative DNS servers were unreachable Thursday morning, he said. Because this DNS information is sometimes cached by ISPs, the NSA would still be temporarily reachable by some users, but unless the problem is fixed, NSA servers will be knocked completely off-line. That means that e-mail sent to the agency will not be delivered, and in some cases, e-mail being sent by the NSA would not get through. "We are aware of the situation and our techs are working on it," a NSA spokeswoman said at 9:45 a.m. PT. She declined to identify herself. A similar DNS problem knocked YouTube off-line in early May. There are three possible reasons the DNS server was knocked off-line, the Arbor Networks representative said. "It's either an internal routing problem of some sort on their side or they've messed up some firewall or ACL [access control list] policy," he said. "Or they've taken their servers off-line because something happened."

Source: <http://www.networkworld.com/news/2008/051508-dns-trouble-knocks-nsa-off.html>

31. *May 15, First Coast News* – (Florida) **Part of Blount Island terminal evacuated.** A portion of the Blount Island terminal in Jacksonville, Florida, was evacuated Thursday due to a bomb squad matter. The Coast Guard says crews found something suspicious near the military cargo area. Authorities set up a safety zone, and the JSO bomb squad and a Navy bomb squad team were investigating. Fifty people who work in two buildings nearby were evacuated.

Source: <http://www.firstcoastnews.com/news/local/news-article.aspx?storyid=109219>

---

## **Emergency Services Sector**

32. *May 15, Rush University Medical Center* – (Illinois) **Mass casualty simulation will better prepare Chicago hospitals' emergency personnel.** Physicians and nurses from hospitals throughout the Chicago area will experience the chaos, confusion and stress of treating a large group of severely injured patients all at once in a unique simulation lab training program at Rush University Medical Center on Wednesday, May 28. The goal of the program is to prepare emergency department personnel from hospitals, large and small, on managing an influx of victims brought in from mass casualty events. The workshop, which will be held in the Rush University Simulation Laboratory, will focus

on creating a realistic, potential situation where a trolley full of passengers explodes and the glass windows of the trolley are blown out as it pulls up to the entrance of Navy Pier on Labor Day. There will be numerous, life-sized computer-controlled ‘virtual patients’ set up to simulate the types of patient cases the trainees may need to triage during a mass casualty scenario. These simulators have life-like human functions that enhance training. They are capable of simulating any possible human medical or traumatic emergency such as loss of limb from a blast injury, penetrating wounds due to the flying glass, open head injuries, penetrating leg injuries, blunt injuries to the head, chest and abdomen, and much more. “The purpose of the exercise is to overwhelm the emergency department personnel with the quantity and severity of casualties with limited time and resources,” said a pediatric critical care physician at Rush University Medical Center.

Source:

[http://www.healthnewsdigest.com/news/Safety\\_310/Mass\\_Casualty\\_Simulation\\_Will\\_Better\\_Prepare\\_Chicago\\_Hospitals\\_Emergency\\_Personnel.shtml](http://www.healthnewsdigest.com/news/Safety_310/Mass_Casualty_Simulation_Will_Better_Prepare_Chicago_Hospitals_Emergency_Personnel.shtml)

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

## **Information Technology**

33. *May 15, InformationWeek* – (National) **Zero-day Internet Explorer vulnerability published.** An Israeli security researcher on Wednesday published details about a zero-day vulnerability in Microsoft Internet Explorer. Last week, the researcher held a “treasure hunt” on his site, where he had hidden the exploit code. He declared “George the Greek” the contest winner in conjunction with the publication of details about the vulnerability. “Internet Explorer is prone to a Cross-Zone Scripting vulnerability in its ‘Print Table of Links’ feature,” he explained in a post on Milw0rm.com summarizing his proof-of-concept exploit. “This feature allows users to add to a printed Web page an appendix which contains a table of all the links in that Web page.” According to the post, an attacker can add a maliciously crafted link to any Web page that accepts user generated content that, under certain circumstances, lets the attacker take control of the user’s machine when he or she tries to print the page. Users of Internet Explorer 7.0 and 8.0b on fully patched Windows XP systems are vulnerable. Users of Windows Vista with User Account Control (UAC) enabled may only be subject to information leakage. Earlier versions of Internet Explorer may also be affected. The researcher said that he alerted Microsoft to the problem on Tuesday and that the company is planning a fix. In the meantime, he advises not using the “Print Table of Links” feature when printing Web pages.

Source:

<http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=207800338>

34. *May 15, vnunet.com* – (International) **Shape-shifting malware hits the web.** Security experts have warned that new developments in malware are allowing criminals to stay one step ahead of security software. The head of the cyber-crime division at the Swiss Justice and Police Department said in an interview last week that viruses and other malware now have the capability to change their signature every few hours. This means that the attackers are often one step ahead of protection software. The chief technology

officer at Tier-3, a behavioral analysis IT security firm, echoed the remarks. “Self-changing code designed to dynamically evade recognition is a fact of life,” he said. “It automatically adapts to the anti-spam and anti-malware engines that it encounters.” Unfortunately the know-how and construction kits used to create this shape-shifting threat are now readily available and are unleashing a wave of malware based on social engineering techniques. “Highly targeted emails containing personalized information and shape-shifting Trojan attachments are the latest development,” he said. “Each positive infection increases the ‘hit rate’ for the next wave of emails sent out by the self-learning automated engines used by sophisticated attackers.” He believes that a non rules-based monitoring process must be set up to defend all ingress and egress points covering SMTP, DNS, HTTP(s), IM etc. “Once this is in place, defense against shape-shifting threats becomes possible as does the removal of any previously established covert data leakage channels that will be revealed and dealt with,” he said.

Source: <http://www.vnunet.com/vnunet/news/2216675/shape-shifting-malware-hits-web>

35. *May 15, Computerworld* – (Texas) **NASA moves to save computers from swarming ants.** A flood of voracious ants is heading straight for Houston, taking out computers, radios and even vehicles in their path. Even the Johnson Space Center has called in extermination experts to keep the pests out of their sensitive and critical systems. The ants have been causing all kinds of trouble in five Texas counties in the Gulf Coast area. Because of their sheer numbers, the ants are short-circuiting computers in homes and offices, and knocking systems offline in major businesses. When IT personnel pry the affected computers open, they find the machines loaded with thousands of ant bodies. “These ants are raising havoc,” said a professor of entomology at Texas A&M University in College Station. “They’re foraging for food, and they’ll go into any space looking for it. In the process, they make their way into sensitive equipment.” The ants have been dubbed Crazy Raspberry ants after Tom Raspberry, owner of Budget Pest Control in Pearland, Texas. He first tackled this particular type of ant back in 2002. Since then, the problem has only escalated. Raspberry told Computerworld that the ants have caused a lot of trouble for one Texas chemical company in particular. Not wanting to name the company, he said the ants shorted out three computers that were running a pipeline that brought chemicals into the plant. The ants took down two computers last year and one in 2006, affecting flow in the pipeline each time. “I think they go into everything, and they don’t follow any kind of structured line,” said Raspberry. “If you open a computer, you would find a cluster of ants on the motherboard and all over. You’d get 3,000 or 4,000 ants inside, and they create arcs. They’ll wipe out any computer.”

Source:

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9086098&intsrc=hm\\_list](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9086098&intsrc=hm_list)

### 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**

36. *May 15, Network World* – (International) **SQL injection attack in ‘third wave,’ says IBM.** A SQL injection attack that has affected at least a half-million Web sites has entered a “third wave” that is more resistant than previous versions to traditional security measures, according to IBM security researchers. “I’ve been tracking SQL injections for the last five or six years. This is some of the most intricate obfuscation I’ve ever seen,” said a research manager for the X-Force technology at IBM’s Internet Security Systems division. A SQL injection is an attack against a database-driven Web site in which the hacker executes unauthorized SQL commands by taking advantage of insecure code on systems connected to the Internet. SQL injections are among the most common Web attacks, partly because a hacker needs little beyond a Web browser and knowledge of SQL queries. These most recent attacks, however, are “extremely complex” and hard to detect until it’s too late, he noted. Hackers are randomly targeting IP addresses throughout the world, looking for any Web site that would accept such an injection, he said. Many successful, widely trusted retail Web sites are being affected. Internet surfers who navigate to infected sites are redirected to “exploitation sites” that simply look broken, with error messages and missing content. The users then are attacked with malware and added to a growing botnet, he says.

Source: <http://www.networkworld.com/news/2008/051508-sql-injection-attack-third-wave.html>

37. *May 15, xchange.com* – (National) **Congress approves Farm Bill, broadband funds included.** Congress today passed a new Farm Bill -- against the threat of a presidential veto -- that would provide loans for rural broadband deployment. The American Cable Association (ACA) welcomed the news. “This bill has traveled a long road, but our hope is that it will have been worth the wait for the unserved communities throughout the country that will benefit from the increased funds and refocused attention of the broadband deployment effort,” said the president and CEO of the ACA. The National Telecommunications Cooperative Association, whose members also include small rural providers, did not immediately return a request for comment. The Farm Bill would, in part, reform the Rural Utilities Service’s Rural Broadband Access Loan and Loan Guarantee Program. That would help providers, co-ops and companies more easily build out in the rural United States.

Source: <http://www.xchangemag.com/hotnews/congress-approves-farm-bill-broadband-funds-.html>

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

## **Commercial Facilities Sector**

Nothing to Report

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

## National Monuments & Icons Sector

38. *May 15, Reuters* – (National) **Coal plant pollution threatens U.S. parks – report.** U.S. regulators are proposing to weaken air quality laws, which would allow new coal-fired power plants to pollute U.S. parks from Shenandoah in Virginia to the Great Basin in Nevada, said the National Parks Conservation Association (NPCA) in its new report. The Environmental Protection Agency has proposed refinements in so-called New Source Review rules that would change the way air pollution is calculated, allowing manipulation by industries seeking pollution permits, the NPCA said. Plans for 28 coal-fired plants threaten the air quality in ten national parks, the report said. The 28 plants would emit annually a combined 122 million tons of carbon dioxide, 79,000 tons of SO<sub>2</sub>, 52,000 tons of NO<sub>x</sub>, and 4,000 pounds of mercury into the air near the ten national parks for at least 50 years, it said. Dirty air in a national park can range from “merely inconvenient,” such as when visitors cannot see more than a few miles due to sooty air, to dangerous, when a child has an asthma attack because of excessive ozone pollution, the report said. Over the long term, the report added, pollution can harm or even kill wildlife in the parks.

Source:

<http://uk.reuters.com/article/oilRpt/idUKN1530011820080515?pageNumber=1&virtualBrandChannel=0>

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

## Dams Sector

39. *May 16, Associated Press* – (Illinois) **Tax to pay for levee repair.** The Illinois House has approved a measure that allows metro-east counties to impose a quarter-cent sales tax to improve Mississippi River levees. The St. Clair County board chairman says the tax is the only way that provides a means to fix the levees. The bill awaits the signature of the state governor, who has not indicated his stand on it.  
Source: <http://www.chicagotribune.com/news/chi-ap-il-leveetax,0,2187923.story>
40. *May 15, Southern Pines Pilot* – (North Carolina) **W.P. Council decides not to revisit dam repair deal.** The Whispering Pines, North Carolina, Council voted 3-2 not to review a previous decision to fix and reopen Martin Way as a part of the Cardinal Lake dam repairs. The council voted last fall in favor of an agreement with Whispering Woods Country Club and local residents to take ownership of the dam and make state-mandated repairs to the dam and Martin Way, the road that runs over the dam.  
Source: <http://www.thepilot.com/stories/20080516/news/local/20080516WPDAM.html>
41. *May 15, White County News* – (Georgia) **Local campsite dam threatens collapse.** Fears of a local dam collapsing have subsided. White County, Georgia, emergency personnel were notified about 5 p.m. Tuesday, May 13, by managers at Camp Barney Medintz of a hole in the private dam at Lake Wendy. The lake is 26 acres in size. “The hole [in the dam] was about six feet in diameter when we got there,” the White County Fire Chief said Wednesday. “It had grown to about 40 feet by the time the lake began to

naturally drain itself. Water is no longer running through the hole in the dam.” The Department of Natural Resources, as well as Georgia Safe Dams representatives, were advised of the situation. Lake owners were expected to secure the cave-in site Wednesday, with lake drainage continuing. While it is uncertain what caused the hole in the dam, the official noted that there is a “probability that the drain pipe that was buried [when the lake was created] corroded to the point that it was allowing the water to wash away the soil.”

Source:

<http://www.whitecountynewstelegraph.com/articles/2008/05/15/news/news03.txt>

42. *May 15, Grand Blanc News* – (Michigan) **More problems arise for Goodrich Dam.**

More damage to Goodrich’s 100-year-old Mill Pond Dam has forced village officials to lower the water level of the pond for a state inspection Tuesday. During a recent village inspection, Department of Public Works employees discovered what a Street Administrator called “a blowout” on the east bank of the dam. Some residents fear the suggestion will include removing the dam and drying out the Mill Pond permanently. The Council President said removing the dam is unlikely.

Source:

[http://www.mlive.com/flintjournal/index.ssf/2008/05/more\\_problems\\_arise\\_for\\_goodri.html](http://www.mlive.com/flintjournal/index.ssf/2008/05/more_problems_arise_for_goodri.html)

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

## **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

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.