



# Department of Homeland Security Daily Open Source Infrastructure Report for 26 April 2007

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](#)

<http://www.dhs.gov/>

## Daily Highlights

- Computerworld reports a new wave of extortion e-mails targeted at higher-income professionals is circulating on the Internet — sent directly to the victims from valid e-mail accounts — that threaten recipients with bodily harm and death if they do not pay thousands of dollars to the sender. (See item [13](#))
- The U.S. Food and Drug Administration says that it will test imports of wheat gluten, corn gluten, corn meal, soy protein, rice bran, and rice protein concentrate to detect any contamination with melamine, which has been found in both human and animal food. (See item [24](#))

## **DHS Daily Open Source Infrastructure Report *Fast Jump***

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

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

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## **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. *April 25, New York Times* — **U.S. takes step to address airliner attacks on reactors.** New nuclear reactors need not be designed to withstand suicide attacks by big airplanes, the Nuclear Regulatory Commission (NRC) decided Tuesday, April 24. Instead, the commission proposed that designers be required to analyze how their reactors can be built to mitigate the effects of such an attack, “to the extent practicable.” The commission has already approved two designs, one by General Electric and one by Westinghouse, for which no such analysis was required.

One design now pending before the commission, a French–German model called the EPR, was devised to meet a European requirement that reactors be built to withstand airplane crashes. And General Electric said Tuesday that it had assessed the capabilities of its two new reactor designs, including the one already approved, and that both “have the capability to withstand the effects of an aircraft crash.” Most of several new designs incorporate features that could be helpful in case of a plane crash, like locating emergency water supplies inside the containment building, at an elevation above the reactor vessel, instead of in a tank outside the building.

Source: [http://www.nytimes.com/2007/04/25/us/25nuke.html?\\_r=1&oref=s\\_login](http://www.nytimes.com/2007/04/25/us/25nuke.html?_r=1&oref=s_login)

2. *April 24, Council on Foreign Relations* — **Report: America’s Vulnerable Energy Grid.** On August 14, 2003, fifty million people in the Northeastern United States and Canada suddenly found themselves without electricity, some for more than twenty–four hours. In July 2006, a nine–day power outage in Queens, New York affected one hundred thousand people. The apparent cause of that disruption was deterioration of the thirty– to sixty–year–old cables servicing the area. The same month, a violent thunderstorm in St. Louis, Missouri knocked out power leaving some seven hundred thousand people without electricity. With an aging infrastructure and growing energy consumption, major outages may become an increasing phenomenon. The specter of terrorism also looms large: Experts say jihadis in Iraq have proven adept at disrupting the electrical grid in that country and could easily apply that same skill set in the United States. Electricity generation and consumption have steadily risen, placing an increased burden on a transmission system that was not designed to carry such a large load. New investments will not alleviate the stress on the transmission grid: While transmission capacity is projected to increase 7 percent in the next decade, demand will rise some 19 percent. As a result, consumers will incur higher costs and blackouts could become more frequent.

Source: <http://www.cfr.org/publication/13153/>

3. *April 24, Associated Press* — **Ethiopian rebels kill 74 in oil attack.** Rebels stormed a Chinese–run oil field near the Somali border on Tuesday, April 24, killing 65 Ethiopians and nine Chinese workers in the dawn raid. The Ogaden National Liberation Front, an ethnic Somali group that has fought alongside insurgents in Somalia, also kidnapped seven Chinese workers, said Bereket Simon, an adviser to the Ethiopian prime minister. “This was a cold blooded killing,” Bereket said. “This was organized.” The rebel group said it had launched “military operations against units of the Ethiopian armed forces guarding an oil exploration site,” in the east of the country. It also warned international oil companies not to operate in the region. Without offering details, the statement said rebels “wiped out” three Ethiopian military units and destroyed the facility. China’s official Xinhua News Agency identified the Chinese workers and Ethiopian guards as employees of the Zhongyuan Petroleum Exploration Bureau, a division of China Petroleum & Chemical Corp., a huge state–run oil company better known as Sinopec. China has increased its presence in Africa in recent years in a hunt for oil and other natural resources to feed its rapidly growing economy. Its forays into areas considered politically unstable, however, has exposed Chinese workers to attacks.

Source: [http://news.yahoo.com/s/ap/20070424/ap\\_on\\_re\\_af/ethiopia\\_china\\_oil\\_attack\\_4;\\_ylt=ArAJqpvt0JUTY5.f3QcArBOAsnsA](http://news.yahoo.com/s/ap/20070424/ap_on_re_af/ethiopia_china_oil_attack_4;_ylt=ArAJqpvt0JUTY5.f3QcArBOAsnsA)

4. *April 23, Associated Press* — **Nuclear plant software contains info available on the Web.** A government Website and public libraries offer some of the information contained in software that a former engineer at the nation’s largest nuclear plant is accused of using while in Iran.

Investigators said they don't believe software engineer Mohammad Alavi intended to provide details of the Palo Verde Nuclear Generation Station to terrorists. Alavi, a native of Iran who is a U.S. citizen, is accused of using the software after he quit working at the plant and while he was in Iran. The training software allows users access to details of plant control rooms and reactors. David Lochbaum, director of nuclear safety for the watchdog group Union of Concerned Scientists, said numerous plant workers already have access to such information and that it could be found in a more fragmented form on a government Website. While operators said the alleged unauthorized use of the software didn't compromise plant security, Arizona Corporation Commissioner Kris Mayes said she wants to meet with plant operators to determine how they will prevent a repeat of the problem.

Source: <http://www.eastvalleytribune.com/story/88363>

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

5. *April 25, TriCities (TN)* — **I-26 shut down due to chemical spill.** Emergency crews closed both northbound and southbound lanes of I-26 near Interstate 81 Wednesday, April 25. Interstate 81 lanes were also closed near the Gray, TN, exit. Authorities said that a holding tank fell from a truck and could be leaking chemicals in that area. Witnesses on the scene also said there was a chemical spill near the Eastern Star exit. The truck is reported to have a 150-gallon holding tank. The chemical in the tank has been identified as sulfur dioxide, a colorless, non-flammable gas that can be life-threatening at levels of high exposure.

Source: <http://www.tricities.com/tristate/tri/news.apx.-content-articles-TRI-2007-04-25-0026.html>

6. *April 19, Dunn Daily Record (NC)* — **Diesel fuel the source of sickness, evacuation.** Diesel fuel being used as a cleaning element on a mop was the source of a strange odor at the Harnett County Governmental Complex Tuesday, investigators say. The incident sent 11 people to the hospital and the employees of three county departments home for an entire day. Harnett County, NC, Public Information Officer Eric Truesdale said investigators discovered diesel fuel on a mop which they believe was used in the health department. Harnett County Director of Emergency Services Gary Pope said the employee put the fuel on a dust mop because the buffer normally used to shine the floors was broken. Investigators evacuated 184 employees from the facility and closed it for the day.

Source: <http://www.dunndailyrecord.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=86681&TM=46525.11>

[[Return to top](#)]

## **Defense Industrial Base Sector**

7. *April 25, U.S. Air Force* — **Air Force officials discuss way forward for new helicopter.** Air Force officials announced in April the way ahead for the replacement combat search and rescue helicopter, the CSAR-X. To foster open communications and a fair and open competition, Air Force officials expect to release a draft Request for Proposal (RFP) amendment to the CSAR-X

offerors in May, and will conduct meetings with the offerors to address comments and answer questions prior to the release of the official RFP amendment.

Source: <http://www.af.mil/news/story.asp?id=123050370>

8. *April 24, CongressDaily* — **Air Force seeks to recover funds diverted to Army.** Air Force Chief of Staff Michael Moseley said Tuesday, April 24, that \$800 million in Air Force funds recently turned over to the increasingly cash-strapped Army will need to be recovered within several months to make his payroll and cover other required personnel costs later this year. "I don't want to have concerns about getting that money back," said Moseley, referring to the Pentagon's unusual request to Congress for permission to transfer \$1.6 billion from Navy and Air Force personnel accounts to pay for the Army's pressing operational needs overseas. Moseley, who warned House appropriators earlier this year against raiding his accounts to pay for the needs of the heavily deployed ground forces, also said he has asked to recover \$1 billion scrubbed from Air Force procurement accounts in the fiscal 2007 wartime supplemental to pay for what the Bush administration calls the "surge" of troops into Baghdad. Moseley estimated the Air Force needs an additional \$20 billion annually to fulfill all requirements. That money, he added, is needed in part to pay for repairing and replacing an aging fleet of aircraft that has significantly declined in readiness over the last several years.

Source: [http://www.govexec.com/story\\_page.cfm?articleid=36709&dcn=to\\_daysnews](http://www.govexec.com/story_page.cfm?articleid=36709&dcn=to_daysnews)

9. *April 24, GovExec* — **Defense procurement chief backs interagency contracts.** Defense procurement officials have been encouraged to weigh all potential contracting vehicles to get the best value on purchases, a senior department official said Monday, April 23. Shay Assad, director of defense procurement and acquisition policy, said in an interview with Government Executive that this includes consideration of interagency contracting shops. The Pentagon spends about \$23 billion annually on interagency contracts, Assad said. A good portion of that is spent on General Services Administration (GSA) schedule contracts. But business with GSA slowed following the discovery of improper contracting practices and misuse of funds at GSA regional offices, and Defense began developing more in-house contract vehicles. Defense and GSA officials signed an agreement in December 2006 to foster better relations. Assad said Monday that the relationship is healthy, but Defense is seeking competition among a variety of contracting entities within and outside the department.

Source: [http://www.govexec.com/story\\_page.cfm?articleid=36706&dcn=to\\_daysnews](http://www.govexec.com/story_page.cfm?articleid=36706&dcn=to_daysnews)

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

## **Banking and Finance Sector**

10. *April 25, Associated Press* — **Dow crosses 13,000 for first time.** The Dow Jones industrial average shot past 13,000 for the first time Wednesday, April 25, powered by signs that the U.S. economy and corporate profits are growing at a steady pace. The stock market's best-known indicator surged past its latest milestone shortly after the opening of trading, and continued rising to 13,036.99 before retracing some of its steps and hovering below the 13,000 mark. Wall Street got an additional lift from the Commerce Department's report of durable goods orders last month, which showed a robust gain in business capital goods. The data reassured investors that demand for U.S. products remains strong, lending support to the economy. The department also reported that sales of new homes rebounded slightly in March, as the market expected. It

took the Dow just 129 trading days, since October 18, to make the trek from 12,000 to 13,000, far less than the 7 1/2 years that the blue chips took to go from 11,000 to 12,000. But the swiftness of this latest trip does recall the days of the dot-com boom when the major indexes were soaring and it took the Dow a mere 24 days to barrel from 10,000 to 11,000.

Source: <http://www.forbes.com/feeds/ap/2007/04/25/ap3650770.html>

11. *April 25, eWeek* — **Neiman Marcus Group data taken via a stolen computer.** The Neiman Marcus Group announced Tuesday, April 25, that "computer equipment owned by a third-party pension benefits plan consultant containing files with sensitive employee information was reported stolen." Neiman Marcus officials said they had no reason to believe the information had been accessed, but they nonetheless are paying for Equifax credit monitoring for any people whose data was on the computer. The company statement said that the computer "contained two-year-old data that was current as of August 30, 2005, and which included the private information of nearly 160,000 current and former Neiman Marcus Group employees and individuals receiving a Neiman Marcus Group pension."

Source: <http://www.eweek.com/article2/0,1895,2121958,00.asp>

12. *April 25, Associated Press* — **Man arrested over 'Bishop' pipe bombs.** An Iowa machinist was arrested Wednesday, April 25, with sending dud pipe bombs and threatening letters to investment companies in Denver and Kansas City in an effort to drive up stock prices. Authorities said he signed the messages "The Bishop." John P. Tomkins, 42, of Dubuque, IA, was arrested on his way to work, and federal agents began searching his home and a storage facility, the U.S. attorney's office said. A criminal complaint unsealed in Chicago charged Tomkins with one count of mailing a threatening communication with intent to extort and one count of possession of an unregistered explosive device. Officials said the pipe bombs would have exploded had just one wire been connected. Investigators have said "The Bishop" mailed more than a dozen letters to financial institutions for 18 months. The letters included references to heaven and hell and threatened recipients if the prices of certain stocks did not move to certain levels, often \$6.66. Tomkins is a former substitute letter carrier who worked weekends for the U.S. Postal Service, authorities said. They said he was not an employee at the time the devices were sent.

Source: [http://www.usatoday.com/news/nation/2007-04-25-bishop-pipebombs\\_N.htm?csp=34](http://www.usatoday.com/news/nation/2007-04-25-bishop-pipebombs_N.htm?csp=34)

13. *April 24, Computerworld* — **A new wave of extortion e-mails circulate the Internet.** A new wave of extortion e-mails that threaten recipients with bodily harm and death if they do not pay thousands of dollars to the sender is circulating on the Internet, according to security vendor SecureWorks Inc. The e-mails are sent directly to the victims from valid e-mail accounts instead of the usual spam relays and bot proxies — an apparent attempt to make them seem authentic. The accounts are set up by scammers purporting to be assassins hired by third parties to harm the recipients. The sender offers to spare the recipient from harm in return for thousands of dollars. About 1,000 of the e-mails have been spotted over the past few days, and they appear to be targeted largely at higher-income professionals such as doctors, lawyers and business owners, according to Don Jackson, a researcher at SecureWorks. The numbers could be higher because many people don't report the e-mails, he said. A similar run of e-mails in December and January prompted the FBI to issue an alert about the scam and urge recipients to simply ignore the messages. The e-mails were sent using popular e-mail services such Gmail,



Yahoo and Hotmail by people believed to be outside the U.S., Jackson said.  
Source: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017723>

[[Return to top](#)]

## **Transportation and Border Security Sector**

**14. *April 25, Government Accountability Office* — GAO-07-623R: Aviation Security: TSA's Change to Its Prohibited Items List Has Not Resulted in Any Reported Security Incidents, but the Impact of the Change on Screening Operations Is Inconclusive (Correspondence).**

The Transportation Security Administration (TSA) has primary responsibility for ensuring the security of civil aviation, which includes the safety of passengers and flight crew. The alleged August 2006 terrorist plot to detonate liquid explosives onboard multiple commercial aircraft bound for the United States from the United Kingdom has highlighted both the continued importance of securing the civil aviation system and the potential that improvised explosive devices may be smuggled onboard passenger aircraft. Based on the Government Accountability Office's (GAO) analysis of TSA data for the third and fourth quarters of fiscal year 2005 (a six-month period), GAO determined that Transportation Security Officers (TSO) spent, on average, less than one percent of their time searching for the approximately 1.8 million sharp objects, other than knives and box cutters, that were found at passenger screening checkpoints between April 2005 and September 2005. With regard to TSA's efforts to increase training for identifying explosives as part of its overall effort to become a more risk-based organization, TSA data between October 2004 and January 2007 show an increase in the average number of hours spent in training per TSO, but there are other factors that may have contributed to this increase.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-623R>

**15. *April 25, Government Accountability Office* — GAO-07-793T: Commercial Aviation: Programs and Options for Providing Air Service to Small Communities (Testimony).**

Congress established two key programs to help support air service to small communities — the Essential Air Service (EAS) providing about \$100 million in subsidies per year and the Small Community Air Service Development Program (SCASDP) that provides about \$20 million per year in grants. As part of its reauthorization of the Federal Aviation Administration (FAA), the Congress is examining the status and outcomes of these programs. This testimony discusses (1) the history and challenges of the EAS program, (2) the implementation and outcomes of the SCASDP and (3) options for reforming EAS and SCASDP. The testimony is based on previous Government Accountability Office (GAO) reports, interviews with Department of Transportation officials and industry representatives as well as program updates.

Highlights: <http://www.gao.gov/highlights/d07793thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-793T>

**16. *April 25, Boston Globe* — MBTA has problems with cracks in its buses.** For the second time in little more than a year, the Massachusetts Bay Transit Authority (MBTA) plans to replace a key part of the rear suspension systems on its 193 low-floor buses, because they are cracking. Starting Wednesday, April 25, state inspectors will conduct independent reviews of the buses as a result of the failures. Any bus not meeting federal safety rules will be pulled from service,

said Timothy J. Shevlin Jr., executive director of the state Department of Public Utilities, which regulates bus safety in Massachusetts. Cracks were first noticed Saturday night during routine maintenance, and by yesterday, mechanics had found cracks or signs of stress in the suspension of at least 22 buses, officials said. They insisted the problem is not a safety issue, but said they plan to repair all 193 buses as a precaution. The new cracks were found in what is called the H-frame, a piece of the suspension system that sits atop the rear axle on four air springs. If the H-frame suffered a catastrophic failure, the bus's rear axle would dip down, but the driver would not lose control, spokesperson Pesaturo said.

Source: [http://www.boston.com/news/local/articles/2007/04/25/t\\_wrestles\\_again\\_with\\_cracks\\_in\\_its\\_buses/](http://www.boston.com/news/local/articles/2007/04/25/t_wrestles_again_with_cracks_in_its_buses/)

17. *April 25, Associated Press* — **Overseas traffic safety concern.** New data being released this week highlights the perils of traffic safety for U.S. travelers abroad. Traffic crashes are the most common cause of non-natural deaths for American tourists, according to Department of State data, more prominent than homicides, acts of terrorism, or natural disasters. Traffic crashes accounted for the deaths of 741 U.S. citizens traveling overseas from 2004–2006, or about one-third of the 2,364 deaths, according to an analysis of State Department data by the Make Roads Safe Campaign, a group funded by automobile clubs dedicated to reducing global traffic deaths and injuries. Traffic safety experts say many American travelers overlook the dangers of road safety during their vacations and need to arrive at their destinations with more than just a packed suitcase, travel papers and vaccinations. They should know about a country's road conditions, look into a travel company's safety record, avoid traveling at night and follow safety standards such as buckling up and not drinking and driving. The report was issued Wednesday, April 25, as part of the first United Nations Global Road Safety Week.

Source: [http://www.usatoday.com/travel/news/2007-04-25-traffic-overseas-safety\\_N.htm](http://www.usatoday.com/travel/news/2007-04-25-traffic-overseas-safety_N.htm)

18. *April 25, Denver Post* — **More bad, some good for United.** United Airlines parent UAL Corp. lost \$152 million in the first quarter, or \$1.32 a share, the company announced on Wednesday, April 25. With increased competition from Southwest Airlines and Frontier Airlines at Denver International Airport, United's revenue performance has suffered in Denver. John Tague, United's chief revenue officer, said, "Clearly we're under pressure in Denver and we expect that to continue." It could mean United will reduce flights in Denver, as the airline plans to reduce domestic capacity. In the domestic market, "We have too much capacity," Tague said. United's loss was worse than analyst expectations.

Source: [http://www.denverpost.com/ci\\_5746931](http://www.denverpost.com/ci_5746931)

19. *April 24, USA TODAY* — **Airline Skybus set to fly in May.** Airline start-up Skybus announced Tuesday, April 24, that it will launch service next month from its Columbus, OH, base, moving discount travel in the U.S. closer than ever to the bare-bones model pioneered by Europe's popular Ryanair. CEO Bill Diffenderffer says the new airline will make its splash in the crowded domestic airline business with ultra-low fares and separate charges for services from baggage handling to onboard snacks. As a permanent pricing feature, Skybus plans to make 10 seats on all flights aboard its 150-seat Airbus A319s available at \$10 each way. Average fares will be pegged at about 50 percent of the going rate of other carriers serving the same markets. Operating from non-congested airports will help keep the carrier's costs, and therefore, its fares, down, Diffenderffer says, as will outsourcing virtually all of its maintenance and ground handling. Beyond the airline's small management team, about the only employees

will be the pilots and flight attendants. Most others will be contract workers. The carrier will begin May 22.

Source: <http://www.usatoday.com/travel/flights/2007-04-24-skybus-lanchn.htm>

20. *April 24, Memphis Business Journal* — **Northwest finalizes Mesaba acquisition.** Mesaba Airlines, which emerged Tuesday from Chapter 11 bankruptcy, has been acquired by Northwest Airlines Corp. and will be its wholly-owned subsidiary, as was previously planned. Mesaba, formerly an independent Northwest Airlink partner owned by MAIR Holdings operates a fleet of 50 regional aircraft. Northwest's other Airlink partner, Memphis-based Pinnacle Airlines Corp., signed a 10-year agreement with Northwest in December 2006, and will remain independent. Mesaba filed for Chapter 11 bankruptcy protection on October 13, 2005, shortly after Northwest had done so. Northwest acquired Mesaba after the airline was "successfully restructured," Northwest said in a statement.

Source: <http://biz.yahoo.com/bizj/070424/1452140.html?v=2>

[[Return to top](#)]

## **Postal and Shipping Sector**

21. *April 25, USPS News Release* — **U.S. Postal Service funds new technologies.** The U.S. Postal Service (USPS) is meeting its performance challenges head on with a \$51 million contract for engineering support services, including support for research and development of new technologies. The contract also provides for technical, project management and IT services, as well as quality assurance consulting work and testing and evaluation of future mail-processing equipment. The contract represents the Postal Service's efforts to continually enhance and develop technologies that improve operational efficiencies and customer service and drive down costs. The two-year base contract has four two-year options, bringing the potential contract value to \$260 million over 10 years.

Source: [http://www.usps.com/communications/newsroom/2007/pr07\\_034.htm](http://www.usps.com/communications/newsroom/2007/pr07_034.htm)

[[Return to top](#)]

## **Agriculture Sector**

Nothing to report.

[[Return to top](#)]

## **Food Sector**

22. *April 24, International Business Times* — **Lexington beef plant remains on list.** The U.S. Department of Agriculture (USDA) has denied a Japanese request to remove a Nebraska processing plant from a list of plants authorized to export beef to Japan. In February, Japan stopped beef imports from a Lexington processing plant operated by Tyson Foods Inc. after finding boxes of beef that had not been verified as from cattle 20 months old or younger, as required by Japan. Japan has been skittish about foreign beef since the first case of mad cow disease was found in the U.S. Although the USDA declined the Japanese request, the Tyson



plant remains under voluntary suspension, said USDA spokesperson Amanda Eamich. Tyson, she said, is fixing the problem, and the shipment in question, while ineligible in part, was inspected and passed before being sent to Japan.

Source: <http://www.ibtimes.com/articles/20070424/japan-us-beef-nebraska.htm>

- 23. April 24, Associated Press — Congress examines food safety cases.** Families victimized by tainted spinach and peanut butter put a human face Tuesday, April 24, on recent high-profile outbreaks of foodborne illness, urging lawmakers to strengthen federal oversight of the nation's food supply. The safety of food raised domestically was questioned anew last fall when officials traced a nationwide E. coli outbreak to contaminated spinach processed by Natural Selection Foods LLC. Three people died and nearly 200 others were sickened. More recently, contaminated peanut butter and pet food have been recalled. Rep. Diana DeGette, D-CO, has introduced legislation that would give the U.S. Food and Drug Administration (FDA) and U.S. Department of Agriculture (USDA) the authority to mandate recalls, in line with a proposal by the Government Accountability Office. Other legislative efforts include proposals to create a single Food Safety Administration and develop a uniform reporting system to track contaminated food. In January, the government's fragmented food safety system joined a congressional "high risk" list, meaning its inefficiencies leave it vulnerable to fraud, waste and abuse. Fifteen federal agencies administer at least 30 laws pertaining to food safety. The FDA, however, is the main food safety agency.

Source: <http://www.abcnews.go.com/Health/wireStory?id=3073809>

- 24. April 24, Reuters — FDA to test food glutens for contamination.** The U.S. Food and Drug Administration (FDA) said on Tuesday, April 24, it will test imports of wheat gluten, corn gluten, corn meal, soy protein, rice bran and rice protein concentrate to detect any contamination with melamine. The materials are used to manufacture both human and livestock feed, the FDA said. "We're going to target firms that we know are receiving imported products," said David Acheson, chief medical officer of the FDA's Center for Food Safety and Applied Nutrition. "The goal is obviously to sample as much as we can."

Source: <http://www.reuters.com/article/healthNews/idUSWBT00687920070424>

- 25. April 24, Associated Press — Hogs ate pet food tainted with chemical.** Salvaged pet food contaminated with an industrial chemical was sent to hog farms in as many as six states, federal health officials said Tuesday, April 24. It was not immediately clear if any hogs that ate the tainted feed then entered the food supply for humans. Hogs at a farm in California ate the contaminated products, according to the U.S. Food Safety and Inspection Service (FSIS). Officials were trying to determine whether hogs in New York, North Carolina, South Carolina, Utah, and Ohio also may have eaten the tainted food, the FSIS said. Hogs at some of the farms, it wasn't immediately clear which, have been quarantined.

Source: <http://www.phillyburbs.com/pb-dyn/news/25-04242007-1335894.html>

[[Return to top](#)]

## **Water Sector**

- 26. April 25, Palm Beach Post (FL) — West Palm Beach shifts to water crisis mode.** Two weeks

ago, with the drought getting worse by the day, West Palm Beach received news from the South Florida Water Management District that sent it scrambling: Water had become so scarce that the city would no longer be able to draw from the L-8 Canal, which is a vital source of water. The city immediately began working on trying to get permission from the district to draw more water from emergency wells. But there's a string attached to that permission, and it has earned the city an unenviable distinction: tighter water restrictions — tighter, even, than the water-only-twice-a-week rule that the rest of Palm Beach County has been ordered to follow. City water officials say the situation is serious. Water experts with the city, water management district, county health department and state Department of Environmental Protection spent several hours Tuesday, April 24, trying to figure out the best way to give West Palm Beach its much-needed water — which sources to use and how much should come from each one. The district also may extend the one-day-a-week restrictions to sprinklers that serve municipal, commercial and industrial landscaping, even though the city exempted them from the toughened rules.

Source: [http://www.palmbeachpost.com/localnews/content/local\\_news/eper/2007/04/25/W1b\\_wpbWATER\\_0425.html](http://www.palmbeachpost.com/localnews/content/local_news/eper/2007/04/25/W1b_wpbWATER_0425.html)

27. *April 25, Associated Press* — **Lye in water blamed for burns, rashes.** Dozens of Spencer, MA, residents were taken to hospitals Wednesday, April 25, with burns or rashes after the town's water supply was accidentally treated with too much corrosive lye, officials said. People in Spencer were advised not to use or touch the water until further notice, said Ed Coletta, a spokesperson for the state Department of Environmental Protection. Residents started complaining of skin irritation and moderate burns after showering early Wednesday, police Sgt. John Agnew said. He said officials determined that a malfunction at the town's water treatment plant had released too much sodium hydroxide into the water supply. Sodium hydroxide, also known as lye, is routinely put into water to reduce acidity and limit pipe corrosion, Coletta said. Source: [http://www.cbsnews.com/stories/2007/04/25/national/main27274\\_81.shtml](http://www.cbsnews.com/stories/2007/04/25/national/main27274_81.shtml)

28. *April 23, Chemical & Engineering News* — **Chemical industry finding ways to secure and expand global water supplies.** The mismatch of water need and abundance reaches across the globe, from developed to developing countries. In the U.S., for example, water levels have dropped dramatically at Hoover Dam and Lake Mead, as a booming population draws heavily on water supplies. Meanwhile, the aquifers of the Great Plains are being depleted by irrigation. Officials in Yemen, on the tip of the Saudi Arabian peninsula, are concerned about the dwindling water reserves supplying the capital city, Sanaa. A rapidly expanding population and increasing use of water for irrigation are fast drawing down the city's water reserves. In fact, officials there are beginning to contemplate moving the historic capital and most of its population to the Red Sea Coast, where desalination could maintain water supplies. Even where there is water, it's often too contaminated to drink without risking serious illness. Seeing both human need and, someday at least, profits, companies in the chemical industry have begun developing a wide range of technologies that can help secure safe drinking water for the world's poor. Usually the projects are offshoots of technology that companies are developing for profit-generating business. Source: <http://pubs.acs.org/cen/coverstory/85/8517cover.html>

[[Return to top](#)]

## **Public Health Sector**

29. *April 25, Reuters* — **Developing countries get help with bird flu vaccine.** Six developing countries, including Indonesia, which has the highest human death toll from bird flu, will get help in making vaccines against the virus, the World Health Organization (WHO) said on Wednesday, April 25. The WHO said Brazil, India, Indonesia, Mexico, Thailand and Vietnam would receive up to \$2.5 million from donations made by the U.S. and Japan. The aim was both to speed the development of new vaccine manufacturing capacity around the world, which is currently far below levels needed to protect the planet's six billion people, and to ease developing country concerns that they might not have rapid access in the event of a bird flu pandemic.

Source: <http://www.alertnet.org/thenews/newsdesk/L25618635.htm>

30. *April 24, University of Nebraska Medical Center* — **Cell suicide theory could provide new hope for fighting antibiotic resistance.** A surprising new theory suggests that some bacterial cells act as “suicide bombers” in cell communities, with the altruistic intention of dying for the common good – and in the process, strengthening other cells that then become resistant to antibiotic drugs. The finding could aid future research into developing drugs that can skirt the potentially catastrophic problem of bacterial resistance to antibiotics. Kenneth Bayles, of the University of Nebraska Medical Center, writes that “programmed cell death” in bacterial communities is a form of altruism that benefits the larger community of cells and helps strengthen them. Three years ago, Bayles began growing cells in biofilm to observe how communication between cells — known as “quorum sensing” — affects their survival. He observed that when cells are forming a biofilm — a colony of bacteria that contains resistant organisms and is involved in many antibiotic-resistant infections — they perform a function that enables them to leave a unique imprint on the world: Their DNA. A small percentage of cells explode in a process called “lysis,” leaving behind a sticky residue that contains DNA and other cellular bioproducts which are then incorporated into the larger cell community to build a stronger biofilm.

Source: [http://app1.unmc.edu/publicaffairs/newsarchive/view\\_art.cfm?article\\_id=1480](http://app1.unmc.edu/publicaffairs/newsarchive/view_art.cfm?article_id=1480)

31. *April 24, Reuters* — **In wake of vaccine, new pneumonia strains emerge.** While a new vaccine has all but eradicated common causes of pneumonia, meningitis and ear infections in children, new strains of bacteria not covered by the vaccine have emerged, U.S. researchers said on Tuesday, April 24. Since the introduction of Wyeth's vaccine Prevnar in 2000, doctors have been waiting and watching for the arrival of replacement bacteria that could undo its progress. Now they may have found it. Researchers from the U.S. Centers for Disease Control and Prevention have noted an increase in the rates of bacterial infections not covered by the current pneumococcal vaccine among native children in Alaska.

Source: <http://www.reuters.com/article/healthNews/idUSN2441376020070424>

[[Return to top](#)]

## **Government Sector**

32.

*April 25, Associated Press* — **Oregon's Rock Creek campus evacuated after threat.** Security officials closed the Rock Creek campus of Portland Community College Tuesday afternoon, April 24, after a threat of violence was discovered. The school also canceled Wednesday's classes. A college spokesperson said a worker found a note in a restroom that threatened violence similar to what occurred at Virginia Tech last week, when a gunman killed 32 people. Deputies conducted a sweep of the campus; no arrests have been made. The threat was the second in a week to close a Portland-area campus.

Source: <http://www.theworldlink.com/articles/2007/04/25/news/news11042507.txt>

[[Return to top](#)]

## **Emergency Services Sector**

**33. *April 24, Federal Emergency Management Agency* — President declares major disaster for New York.** The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Tuesday, April 24, that federal disaster aid has been made available for the state of New York to help people and communities recover from the effects of severe storms and inland and coastal flooding during the period of April 14–18, 2007. FEMA Administrator David Paulison said the assistance was authorized under a major disaster declaration issued for the state by President Bush. The President's action makes federal funding available to affected individuals in Orange, Rockland and Westchester counties.

Source: <http://www.fema.gov/news/newsrelease.fema?id=35651>

**34. *April 24, Associated Press* — Rescuers often can't find 911 callers.** A new report by a public safety group throws into question the ability of police and firefighters to locate people through their cell phones when they dial 911 in an emergency. The study is believed to be the first independent evaluation of wireless location technology and sends a clear message: Do not assume rescuers will know where you are if you call 911 from a cell phone. The report was commissioned by the Association of Public Safety Communications Officials International, a group that has long been concerned about the limitations of the technology and the public's unrealistic expectations of what it can deliver. The Associated Press was given an advance copy of the study, which will be officially released in May. While the report pointed out the generally poor performance of the wireless industry in locating 911 callers, it also pointed out a need for 911 call centers to work closely with providers and the importance of public education. A new generation of telephone customers is being raised without using land-based telephone lines. But they still expect rescuers to be able to find them.

Source: [http://news.yahoo.com/s/ap/cell\\_phones911;\\_ylt=AiDD\\_TVK2WCgcKBpP3MhfKwjBAF](http://news.yahoo.com/s/ap/cell_phones911;_ylt=AiDD_TVK2WCgcKBpP3MhfKwjBAF)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

**35. *April 25, U.S. Computer Emergency Readiness Team* — Vulnerability in HP-UX running sendmail.** The U.S. Computer Emergency Readiness Team (US-CERT) is aware of a vulnerability in HP-UX running sendmail that may allow a remote user to cause a

denial-of-service condition. US-CERT recommends users apply the patches as described in HP Technical Knowledge Base Document c00841370. Please note that logon credentials may be needed to access this document. US-CERT will continue to investigate this issue and provide additional information as it becomes available.

HP Technical Knowledge Base Document c00841370:

<http://www2.itrc.hp.com/service/cki/docDisplay.do?docId=c00841370&admit=-1335382922+1177517201483+28353475>

Source: [http://www.uscert.gov/current/#hp\\_ux\\_sendmail\\_vulnerability](http://www.uscert.gov/current/#hp_ux_sendmail_vulnerability)

36. *April 25, IDG News Service* — **Microsoft ups security stance with new labs.** In a move to strengthen its response to security threats, Microsoft is opening two labs to study the growing amount of malicious software circulating on the Internet, security executives announced Wednesday, April 25. The Malware Protection Centers, in Dublin and Tokyo, will be staffed with analysts who will create updates -- called "signatures" -- for its security products to detect malicious software, said Roger Halbheer, chief security advisor for Europe, the Middle East and Africa. The labs will be similar to ones run by competitors such as Symantec and McAfee.  
Source: [http://www.infoworld.com/article/07/04/25/HNmssecuritylabs\\_1.html](http://www.infoworld.com/article/07/04/25/HNmssecuritylabs_1.html)
37. *April 25, IDG News Service* — **'Evil twin' Wi-Fi access points proliferate.** Beware of the "evil twin." That's the term for a Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers. Unfortunately, experts say there is little consumers can do to protect themselves, but enterprises may be in better shape. With the growth in wireless networks, the "evil twin" type of attack is on the rise, said Phil Cracknell, president of the UK branch of the Information Systems Security Association. Such attacks are much easier than others seeking logins or passwords, such as phishing, which involves setting up a fraudulent Website and luring people there, Cracknell said. The growth in the number of Wi-Fi networks poses increasing opportunities for hackers, who can make their networks appear to be legitimate by simply giving their access point a similar name to the Wi-Fi network on the premises.  
Source: [http://www.infoworld.com/article/07/04/25/HNevilwifiaccesspo\\_ints\\_1.html](http://www.infoworld.com/article/07/04/25/HNevilwifiaccesspo_ints_1.html)
38. *April 25, VNUNet* — **Rogue software floods anti-spyware market.** Malware writers are flooding the market with rogue anti-spyware applications in an attempt to steer consumers away from genuine security software and make money from selling bogus applications. Download service Snapfiles said that the rogue applications outnumber genuine software by a factor of four to one. Snapfiles hosts free and trial applications for consumers to download, and claims to reject any software that fails to deliver the promised functionality or causes harm to a system. Download site Tucows confirmed the figure, saying that it too rejects about four-fifths of the anti-spyware programs it receives from developers. Rogue anti-spyware programs present themselves as legitimate security solutions, but have no intention of ridding a user's system of malware. Instead, the application scares the user with false test results, fails to get rid of existing spyware infections, and in some cases even infects the system with additional pieces of spyware and adware.  
Source: <http://www.vnunet.com/vnunet/news/2188549/rogue-apps-dominat ing>



39. *April 24, Associated Press* — **Researchers break Internet speed records.** A group of researchers led by the University of Tokyo has broken Internet speed records — twice in two days. Operators of the high-speed Internet2 network announced Tuesday, April 24, that the researchers on December 30 sent data at 7.67 gigabits per second, using standard communications protocols. The next day, using modified protocols, the team broke the record again by sending data over the same 20,000-mile path at 9.08 Gbps.  
Source: [http://www.nytimes.com/aponline/technology/AP-Faster-Internet.html?\\_r=1&oref=slogin](http://www.nytimes.com/aponline/technology/AP-Faster-Internet.html?_r=1&oref=slogin)
40. *April 24, CNET News* — **Web threats to surpass e-mail pests.** By next year, Internet users can expect more cyberattacks to originate from the Web than via e-mail, security firm Trend Micro predicts. E-mail has traditionally been the top means of attack, with messages laden with Trojan horses and other malicious programs hitting inboxes. But the balance is about to tip as cybercrooks increasingly turn to the Web to attack PCs. "By 2008, most of the threats you are facing will be Web placed. Today most of it is still e-mail," Raimund Genes, Trend Micro's chief researcher, said in a presentation at the Gartner Symposium and ITxpo on Monday, April 23. The reason for the flip is simple. Security tools for e-mail have become commonplace, but the same isn't true for Web traffic. Security firms have found it tough to secure what comes into a network and computers over port 80, the network port used to browse the Web using the hypertext transfer protocol, or HTTP.  
Source: [http://news.com.com/Web+threats+to+surpass+e-mail+pests/2100-7349\\_3-6178930.html](http://news.com.com/Web+threats+to+surpass+e-mail+pests/2100-7349_3-6178930.html)

### 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: [www.us-cert.gov](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/>.

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

## Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

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

## General Sector

Nothing to report.

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

## **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 [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.osis.gov](mailto:dhsdailyadmin@mail.dhs.osis.gov) or contact the DHS Daily Report Team at (703) 983–3644 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.