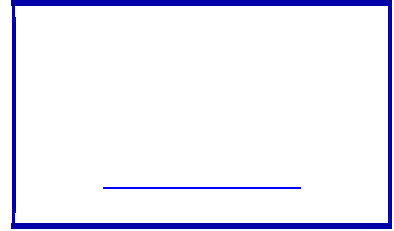




Department of Homeland Security Daily Open Source Infrastructure Report for 11 April 2008



- The Asbury Park Press reports heightened awareness has increased the distribution of potassium iodide pills that could protect people's thyroids from radiation near the Oyster Creek nuclear power plant in Lacey, New Jersey. (See item [27](#))
- According to the Associated Press, China said Thursday it had uncovered a criminal ring planning to kidnap athletes, foreign journalists, and other visitors at the Beijing Olympic Games. Thirty-five members of a ring based in the restive western Xinjiang region were arrested between March 26 and April 6. (See item [38](#))

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. *April 10, Agence France-Presse* – (International) **Oil prices soar after hitting 112 dollars.** World oil prices rallied on Thursday, after striking an all-time record above \$112 per barrel when the market was lifted by tumbling U.S. energy reserves and weakness of the dollar, traders said. New York's main oil contract, light sweet crude for delivery in May, gained 99 cents to \$111.86. The contract had rocketed to a record \$112.21 on Wednesday. Crude futures had soared by more than three dollars on Wednesday after the U.S. Department of Energy (DOE) reported that American energy stockpiles fell across the board during the week ending April 4. U.S. crude reserves slumped by 3.2 million barrels and gasoline or petrol inventories shed 3.4 million

barrels, the DOE said.

Source: <http://afp.google.com/article/ALeqM5hAelEboBEFrk16DjkOwKG8RCeOTw>

2. *April 10, Associated Press* – (Arkansas; Oklahoma; Texas) **Storms cut power across central U.S.** A band of hail, heavy rain and twisters pounded Arkansas, Texas, and Oklahoma, damaging hundreds of homes, flooding roads, leaving tens of thousands without power, and claiming at least one life. Arkansas was bracing for more severe weather later in the day. At least 180,000 homes and businesses lost electricity in the Dallas-Fort Worth, Texas, area, and more than 11,000 customers were without power in Oklahoma Thursday morning.

Source: <http://www.msnbc.msn.com/id/24040801>

3. *April 9, Dow Jones Newswires* – (Southeast) **Independence Hub to restart in 1-to-4 weeks: Enterprise.** Gas production at the Independence Hub gas platform in the U.S. Gulf of Mexico is expected to restart production in one-to-four weeks, Enterprise Products Partners' said Wednesday afternoon in a news release. A leak was suspected Tuesday in the 134-mile-long Independence Trail pipeline, after Anadarko Petroleum Corp. workers noticed bubbles coming up from the ocean. The leak was confirmed by a remote-operated vehicle Wednesday morning. Enterprise is in the process of rounding up the necessary equipment and personnel including to make repairs, said an Enterprise spokesman. "Based on initial findings and the scope of work, repairs could take anywhere from one to 4 weeks," he said.

Source:

http://money.cnn.com/news/newsfeeds/articles/djf500/200804091544DOWJONESDJONLINE000987_FORTUNE5.htm

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

Chemical Industry Sector

4. *April 9, Associated Press* – (Tennessee) **Eastman Chemical, state regulators say no harm by chemical spill.** Regulators and company officials say a minor chemical spill at the Eastman Chemical Co. plant in Kingsport, Tennessee, caused no harm to the environment. The spill occurred Friday when one of the company's vessels overheated. About 160 gallons of a chemical identified by its brandname as DowTherm was released to relieve pressure. Employees sprayed water on the material and the diluted mixture washed into the Holston River, where it dissipated. Dow Chemical Co. describes DowTherm on its Web site as a glycol-based heat transfer fluid that is formulated with heavy-duty industrial inhibitors to prevent corrosion. "There was no impact on the environment. No fish kill. No harm to humans or nature," an Eastman spokeswoman said Wednesday. The Tennessee Department of Environment and Conservation monitored the incident and told the Kingsport Times-News there was no danger to the environment.

Source: <http://www.knoxnews.com/news/2008/apr/09/eastman-chemical-state-regulators-say-no-harm-chem/>

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

Nuclear Reactors, Materials, and Waste Sector

5. *April 10, Associated Press* – (Washington) **Probe sought in lapses at Hanford waste plant.** About 1,800 sections of pipe for a massive waste-treatment plant at the nation's most contaminated nuclear site were not subjected to required quality inspections, and a U.S. senator has called for a full explanation by the government agency overseeing the project. The Hanford nuclear reservation plant is under construction in south-central Washington by Bechtel National. Bechtel's communications manager said none of the pipe in question was permanently installed in the building, and most were drain pipes that will not carry waste or be subject to high pressure or high temperatures. Bechtel's workers identified the problem themselves and are taking steps to prevent a recurrence. In a letter to the U.S. Energy Department secretary, a U.S. senator requested an explanation of the cause of the problems and assurance that steps are being taken to address inadequate construction management.
Source: http://seattletimes.nwsources.com/html/localnews/2004339019_hanford10m.html
6. *April 10, Solanco News* – (Pennsylvania) **NRC to discuss results of safety conscious work environment inspection at Peach Bottom.** U.S. Nuclear Regulatory Commission (NRC) officials will meet with Exelon Generation Co. representatives on Tuesday, April 15, to discuss the results of a "safety conscious work environment" inspection conducted at Peach Bottom, which is located in Delta, Pennsylvania. The inspection was conducted by six NRC inspectors during the week of March 24. Following the discussion of the NRC inspection findings, Exelon will discuss the status of the "safety conscious work environment" surveys it plans to conduct at its nine other operating reactor sites.
Source: http://www.solanconews.com/Gov/Articles/2008/080410_NRC_peachbottom.htm
7. *April 9, Associated Press* – (Utah) **Hill AFB: Trace amounts of depleted uranium burned.** Military officials say trace amounts of depleted uranium were incinerated during the destruction of classified components at a burn plant near Layton, Utah. Hill Air Force Base (AFB) officials say less than five pounds of depleted uranium were burned over eight months before it was discovered last month that the parts contained the material. The military says there were no public health, safety, or environmental risks. Crews conducting the work were not aware the parts contained depleted uranium because the 40-year-old drawings and other information describing the components were not readily available. Hill AFB officials said they also met with health officials, elected leaders, and others to discuss the releases. Base officials say engineers at the plant are now looking at other ways to destroy the components.
Source: <http://www.localnews8.com/Global/story.asp?S=8144102>
8. *April 9, Ocala Star-Banner* – (Florida) **Crystal River nuclear plant earns good safety marks.** Progress Energy Florida received good marks Tuesday from the U.S. Nuclear Regulatory Commission (NRC) for its 2007 safety record at its Crystal River nuclear power plant. Progress Energy executives are hoping the good safety record demonstrates the company's ability to operate a second plant, which it hopes to build in Levy County.

The 31-year-old Crystal River plant had only seven violations in 2007, and all of those were the least serious possible according to standards set by the NRC, said an onsite plant inspector for the agency. Despite the accolades for its safety record, Crystal River's plant site vice president said during Tuesday's annual safety performance report meeting that the plant still had some problems it wanted to resolve. When plant workers exchanged radioactive fuel rods last year, the plant exposed workers to 185 REMS, a unit of radiation exposure. The plant's standard is for no more than 140 REMS. None of the radiation left the plant, the vice president said, "but we have some work to do during outages and repairs."

Source:

<http://www.ocala.com/article/20080409/NEWS/804090323/1001/NEWS01&tc=yahoo>

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

Defense Industrial Base Sector

9. *April 9, Reuters* – (National) **Military's space demands keep topping supply.** U.S. military demand for satellite services will continue to outrun supply as the U.S. fleshes out a global information "mosaic," said the Air Force secretary at the National Space Symposium Wednesday. U.S. defense contractors are vying for billions of dollars of work on advanced military communications, navigation, and other satellite systems that will boost U.S. signal-processing power as much as ten-fold compared with systems being replaced. In the meantime, Intelsat and Americom Government Services provide as much as 80 percent of the bandwidth to the U.S. military, according to Futron Corp. Since 2001, funding for Air Force space programs has nearly doubled for everything from monitoring weather to intelligence, surveillance, and reconnaissance. The commander of the Space Command's satellite-buying Space & Missile Systems Center said compromises were constantly made because of the crunch. The Air Force secretary said the U.S. also must do more to protect space assets on which it relies for a large and growing list of commercial and civilian needs. "While we have made considerable progress in fielding space capabilities, we have not sufficiently addressed space survivability among many of our space systems," he said.

Source:

http://news.yahoo.com/s/nm/20080409/us_nm/space_usa_dc;_ylt=AmGUH52ZLzBzAeRfIzaUIKwWIr0F

10. *April 9, Defense News* – (National) **USAF joins Navy in warning of 'fighter gap.'** U.S. Air Force and Navy officials gave Congress a bleak assessment of the Pentagon's future fighter fleet, warning lawmakers the military might be 900 fighter jets short of what it will need around 2020. Senior naval officials in the last few months have talked publicly about a "fighter gap" between 2015 and 2025, during which time they say the Navy will be short of the planes they expect would be needed for the Navy to carry out possible missions. During an April 9 Senate Armed Services airland subcommittee hearing, the director of the service's air warfare division indicated the sea service's gap could be about 70 planes deep. A senior Air Force official indicated his service could face an even larger deficit of needed fighters, possibly as large as "over 800 fighters" between 2017 and 2024. While attempting to get a grasp on how it can manage its "fighter gap,"

Navy officials have floated the idea of delaying its version of the F-35 in favor of buying new – and upgrading older – Boeing-made F/A-18 Hornets. The Air Force already has launched its own review to determine how many legacy F-15s and F-16s it might have to try and keep operationally fit to help manage its perceived fighter deficit. The military deputy to the Air Force’s acquisition chief told the subcommittee a decision is needed on whether the service will be granted a budget plus-up for more F-22As by November.

Source: <http://www.defensenews.com/story.php?i=3472033&c=AME&s=AIR>

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

Banking and Finance Sector

11. *April 10, Associated Press* – (National) **Report: IRS not doing enough on ID theft.**

Tax-fraud identity theft will be the subject of a Thursday Senate hearing. A Treasury Department report says the number of phony tax returns filed as a result of identity theft has jumped more than six times over the past five years. But the report also notes that the Internal Revenue Service rarely pursues or prosecutes such cases. The report by Treasury’s inspector general says the main incentives for stealing a person’s Social Security number and taxpayer identity are to steal a tax refund through a fraudulent return or to get a job. The report says that between 2002 and 2007 the number of fraudulent tax-return complaints to the Federal Trade Commission soared from 3,000 to more than 20,000.

Source: <http://www.localnews8.com/global/story.asp?s=8145566&ClientType=Printable>

12. *April 10, Wheeling Countryside* – (National) **Tax return shouldn’t be outsourced overseas.**

Before engaging a tax preparer, the Better Business Bureau advises people to ask who will actually prepare their return. Customers should determine if the preparer is exporting their return to a foreign country for preparation. Foreign countries do not have the same security and privacy laws as the United States, nor is there any recourse should customers’ information be compromised as a result of lax or nonexistent privacy procedures. People should also beware of a preparer who guarantees results or who bases fees on a percentage of the amount of the refund. A practitioner may not charge a contingent fee (percentage of the refund) for preparing an original tax return. Tax payers should investigate whether the preparer has any questionable history with the Better Business Bureau, the state’s board of accountancy for CPAs, the state’s bar association for attorneys or the IRS Office of Professional Responsibility for enrolled agents, or the oversight agency in states that license or register tax preparers.

Source: <http://www.pioneerlocal.com/wheeling/business/883738.pp-bbb-041008-sl.article>

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

Transportation Sector

13. *April 10, Associated Press* – (National) **Frustration continues as American Airlines cancels more than 900 flights Thursday.** American Airlines canceled more than 900

flights Thursday to fix faulty wiring in hundreds of jets, marking the third straight day of mass groundings as company executives offered profuse apologies and travel vouchers to calm angry customers. American, the nation's largest carrier, has now scrubbed more than 2,400 flights since Tuesday, when federal regulators warned that nearly half its planes could violate a safety regulation designed to prevent fires. That's more than one in three flights canceled over the last three days. An executive vice president of American said cancellations could extend into Friday. A return to normal operations depends on how quickly mechanics can inspect and fix the wire bundles. An airline spokesman said late Wednesday afternoon that 60 planes had been cleared to fly, 119 were being worked on, and 121 planes had not yet been inspected. American estimates that more than 100 passengers would have been on each of those canceled flights. That means a quarter-million people have been inconvenienced this week. American declined to say how much it would spend on \$500 travel vouchers and hotel rooms for stranded travelers and overtime for mechanics, or how much revenue it would lose by putting some displaced customers on other airlines.

Source: <http://www.foxnews.com/story/0,2933,349189,00.html>

14. *April 10, ABC News* – (National) **How old is that plane you're boarding?** Travelers are confronting another miserable day at the nation's airports Thursday, as American Airlines anticipates more than 900 cancellations. Now industry experts say several of the airlines' problems are rooted in one underlying issue: aging planes. Those recently reinspected are some of the oldest planes that U.S. airlines are flying today. Of roughly 4,400 airplanes worldwide that are 21 years or older, half of those are in the United States, according to an analyst with Friedman, Billings, Ramsey & Co., who follows the airplane leasing business. While the planes may be safe, the older they get the more likely they are to have maintenance problems, causing another catastrophic delay. Still, faced with financial struggles, U.S. carriers have no major public plans so far to replace their older aircraft. But as U.S. carriers hold off on the upgrades, foreign carriers are investing in improvements. But even if U.S. airlines wanted to replace their old jets with new fuel-efficient ones, the analyst said the average backlog is about six years. Those already in line for the planes are airlines from Brazil, Russia, China and India.
- Source: <http://abcnews.go.com/Business/BusinessTravel/story?id=4622145&page=1>

15. *April 10, USA Today* – (National) **TSA unveils plan to X-ray air cargo.** The Transportation Security Administration is launching a program that for the first time aims to screen all cargo on passenger airplanes. The effort begins this summer in major cities and could lead to longer delivery times for packages shipped through the air. It seeks to close a hole that allows millions of packages to be carried under passenger cabins without being checked for bombs. Manufacturers such as Dell and others rely on passenger planes to deliver tons of freight, such as computers and auto parts, to retailers. A key part of the plan is that it will rely on packing companies to volunteer to screen cargo they deliver to airports. Companies that sign up will have to buy and run screening machines and face TSA regulation -- which could deter volunteers. The move to screen the 250 million freight packages carried each year by passenger airlines comes after government audits criticized cargo security. The TSA uses a computer to identify packages for scrutiny, and requires passenger airlines to screen some cargo. Cargo

airlines, which carried 93 percent of the 27 billion pounds of air freight in 2007, are not part of the TSA's new effort and are seen as less of a terrorist target. U.S. mail on passenger planes also is excluded. A law enacted last year requires that all passenger-plane cargo be screened, starting in 2010.

Source: http://www.usatoday.com/news/nation/2008-04-09-Aircargo_N.htm?csp=15

16. *April 10, Business Week* – (National) **The offshoring of airplane care.** As airlines scramble to cut costs, outsourced repair shops -- both in the U.S. and abroad -- now handle two-thirds of all maintenance for American carriers, the U.S. Transportation Department says, up from 30 percent in 1997. Airline maintenance has become a \$42 billion-a-year business, with countries such as Dubai, China, Korea, and Singapore making enormous investments to attract such work. While there is some concern about the 4,181 maintenance operations in the U.S., the bigger worry is over the 700-plus foreign shops overseen by the Federal Aviation Administration (FAA). Beyond those, there are numerous other shops not certified by the FAA that offer airlines various maintenance services. Airlines are entrusting vital work, critics say, to companies abroad that the FAA does not have the resources to monitor effectively. Even those overseas facilities that the agency visits do not have to conduct the criminal-background checks and random drug and alcohol tests on aircraft mechanics that are required at domestic facilities. And it is difficult for the FAA to stage surprise inspections, as it does in the U.S. Members of Congress and industry watchdogs have stepped up calls for greater FAA inspections of repair shops abroad so they meet U.S. standards. The House of Representatives has approved a bill requiring drug and alcohol testing for overseas maintenance workers, as well as twice-yearly FAA inspections. The Senate has yet to move on the issue. In this environment, some airlines are reconsidering their maintenance operations. On April 3, Southwest said it would keep all of its repairs in the U.S. rather than ship some of them, as planned, to Aeroman.

Source:

http://www.businessweek.com/bwdaily/dnflash/content/apr2008/db2008049_205948.htm?chan=top+news_top+news+index_businessweek+exclusives

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

Postal and Shipping Sector

17. *April 10, Macon Telegraph* – (Georgia) **Suspicious package at RAFB prompts evacuation.** Discovery of a suspicious package prompted the evacuation of some buildings at Robins Air Force Base, Georgia, on Wednesday morning, a base spokesman confirmed. The package was discovered at the base post office about 9:30 a.m., said the chief of media relations for the 78th Air Base Wing. As a precaution, several buildings were evacuated. Base officials declined to disclose what was in the package, but the incident was over within an hour.

Source: <http://www.macon.com/197/story/318832.html>

18. *April 9, WAPT 16 Jackson* – (Mississippi) **FBI investigating 'suspicious substance' at federal building.** The Federal Bureau of Investigation (FBI) is investigating a "suspicious substance" that led to the evacuation of the Federal Building in Jackson,

Mississippi, Wednesday afternoon. An Internal Revenue Service employee opened a box or a package containing a white powder, according to Jackson Fire officials. The woman began itching and sneezing, said an employee of the General Services Administration. The woman has been evaluated and is being treated at a local hospital. Officials are treating the substance as a possible hazard. Officials could not immediately say what the powder was. The FBI and the U.S. Occupational Safety and Health Administration are investigating the incident. Jackson Fire Department Haz-Mat crews, Jackson Police, and American Medical Response ambulances are also on the scene. Source: <http://www.wapt.com/news/www.wapt.com/news/15837295/detail.html>

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

Agriculture and Food Sector

19. *April 9, Reuters* – (National) **As grain growers profit, U.S. hog farmers suffer.** High prices for grains, driven by demand for food around the world, means high prices for hog feed. The price of energy, a major cost for farmers, has also jumped, and hog prices have dropped well below production costs for farmers all over the U.S. Economists predict that some will pare back this year and others will quit. Smithfield Foods Inc., the country's largest hog producer, has already said it is cutting production because of high feed costs. An agricultural economist at the University of Missouri predicts producers will lose money throughout 2008 and much of 2009.

Source:

http://news.yahoo.com/s/nm/20080410/us_nm/usa_farm_hogs_dc;_ylt=Am4HioNbt2pWh7GIW6P6lGMWlr0F

20. *April 9, Meatingplace.com* – (National) **USDA to start testing for non-O157 E. coli in beef.** The U.S. Department of Agriculture plans to start testing ground beef and ground beef component samples for non-O157 Shiga Toxin-Producing E. coli (STECs) to determine whether to declare them adulterants. Officials from USDA's Food Safety and Inspection Service told participants at a meeting on Wednesday the agency will test both samples that test positive and those that test negative for E. coli O157:H7, but production lots will not be recalled, seized or detained if they only test positive for non-O157 STECs. The data is being generated only for study purposes at this time. The USDA will issue a public notice to announce a start date, which has not been determined. The FSIS Deputy Assistant Administrator said the agency will assess the testing data "over a limited timeframe sufficient to ascertain the general likelihood of the presence of selected non-O157 STECs. Based on the evidence that we develop from our testing, as well as other available evidence, we will decide whether to declare selected non-O157 STECs to be adulterants," he said in a presentation prepared for the group. Well aware of the controversy these and other proposed actions are likely to generate, FSIS' Under Secretary opened the meeting by saying, "You certainly may hear things you don't agree with...Progress won't occur if we're just wanting to avoid discomfort by maintaining the old status quo. The E. coli bug is obviously not satisfied with the status quo and neither should we be."

Source: <http://www.cattlenetwork.com/content.asp?contentid=212042>

21. *April 9, Feedstuffs* – (National) **Latest USDA report shows tighter supplies ahead.** Thursday morning, the U.S. Department of Agriculture updated its World Agricultural Supply and Demand Estimates (WASDE) indicating tighter world supplies ahead. U.S. corn ending stocks for 2007/08 are projected 155 million bushels lower this month, 65 million bushels lighter than the average trade guess, as increases in feed and residual use and exports more than offset a reduction in corn use for ethanol. Feed and residual use is projected 200 million bushels higher as March 1 stocks indicated higher-than-expected disappearance during the December-February quarter. Ethanol corn use is projected 100 million bushels lower as the pace of new plant startups lags earlier expectations; however, rising ethanol prices continue to support producer margins and capacity utilization for existing plants remains strong. Exports are projected 50 million bushels higher based on the strong pace of shipments and large outstanding sales balances. The market continues to try and bid up prices to buy at least 3 million more corn acres to meet growing world corn demand, creating continued volatility in the corn market, an analyst said.
Source:
<http://www.feedstuffs.com/ME2/dirmod.asp?sid=F4D1A9DFCD974EAD8CD5205E15C1CB42&nm=Breaking+News&type=news&mod=News&mid=A3D60400B4204079A76C4B1B129CB433&tier=3&nid=8DAAD9A58067409CB655DEBF8491959F>
22. *April 9, United Press International* – (National) **USDA cites 4 plants for inhumane treatment.** Four of 18 beef slaughterhouses supplying meat to U.S. school lunch programs were cited for inhumane treatment of cattle, a federal report to Congress said on Wednesday. The U.S. Agriculture Department's audit released to Congress indicated one slaughterhouse was temporarily closed. Congress sought the audit after the shutdown of Westland/Hallmark Meat Packing Co. of Chino, California, a school lunch supplier cited for violating health rules on humane handling of animals. A USDA letter to the chair of a Senate agriculture subcommittee, said the unnamed plant did not effectively stun cattle on the first attempt before slaughter. The plant corrected the problem and lost about a half day of production, a USDA spokeswoman said. The USDA letter said the 17 other plants had "acceptable humane-handling programs and practices." It cited one facility for cattle overcrowding, one for excessive use of stunning prods, and one for conditions allowing excessive hesitation by cattle as they neared the stun box. The audit indicated the likelihood other slaughterhouses have problems, animal advocates say.
Source:
http://www.upi.com/NewsTrack/Top_News/2008/04/09/usda_cites_4_plants_for_inhumane_treatment/3775/

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

Water Sector

23. *April 10, Orlando Sentinel* – (Florida) **Osceola County joins fight over St. Johns River water.** Osceola County, Florida, has joined the water war over the St. Johns River. A Tallahassee judge this week approved requests by Osceola and its Tohopekaliga Water Authority to enter the fray over pumping water out of the St. Johns

river. The case is about Seminole County's proposal to take 5.5 million gallons daily from the river for irrigation, a plan opposed by Jacksonville-area communities and environmentalists. Osceola County barely borders the 310-mile river, but officials at the county and the Toho utility think a victory by the northeast Florida coalition could jeopardize a separate and much more ambitious proposal by Osceola, Orange, Orlando, and others to cooperate in using river water. North Florida fears that using the St. Johns River as a water source will harm its ecosystem. The river flows north from central Florida through Jacksonville to the Atlantic Ocean. The St. Johns River Water Management District wants central Florida to consider pumping as much as 250 million gallons daily from the river and its tributaries. That is because the traditional water supply – the underground Floridan Aquifer – cannot give more water without becoming contaminated by saltwater and without draining springs, wetlands, and rivers.

Source: <http://www.orlandosentinel.com/news/local/osceola/orl-waterwar1008apr10.0.6095132.story>

24. *April 9, Sacramento Bee* – (California) **U.S. to pay \$250,000 over groundwater pollution.** The federal government has agreed to pay California-American Water Co. \$250,000 to defray the company's costs of cleaning up hazardous waste found in one of its drinking water wells in Rancho Cordova. The government has also agreed to undertake renewed testing at the well and, if further pollution at a certain level is detected, provide treatment of the water at the wellhead or an alternative source of clean water. The well was fouled by groundwater pollution emanating from the former Mather Air Force Base. The pact's terms are set out in a consent decree that Cal-Am and the government are asking a U.S. district judge to approve and in a separate settlement agreement. The judge's approval of the consent decree would resolve a legal dispute that began in November 2005 when Cal-Am sued the federal government to recover its costs. The government later countersued.

Source: <http://www.sacbee.com/101/story/848796.html>

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

Public Health and Healthcare Sector

25. *April 10, Washington Post* – (National) **Stolen NIH laptop held social security numbers.** Social Security numbers for more than 1,200 participants in a National Institutes of Health (NIH) study were stored on a stolen laptop containing their medical records, putting those patients at risk of identity theft, agency officials said. They had initially assured the more than 3,000 patients whose records were on the laptop that the computer's contents – unencrypted, in violation of federal policy – did not contain any information that could put their identity or finances at risk. However, an ongoing review of the computer's last-known contents, performed on data backed up from the laptop before the theft, found a file that included Social Security numbers for at least 1,281 of the 3,078 patients enrolled in a multi-year study, which is sponsored by the NIH's National Heart, Lung and Blood Institute. The file had been loaded onto the laptop by a research associate, unbeknownst to the lead researcher. An NIH spokesman said Wednesday that letters are being sent to all those affected, informing them of the risk and offering them free registration for a service that will allow them to monitor their

credit reports. The NIH is also insuring each participant for up to \$20,000 in losses from identity theft. The cost to taxpayers for those services is estimated to be \$18,400.

Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/04/09/AR2008040903680_pf.html

26. *April 10, Philadelphia Business Journal* – (Pennsylvania) **Pa. had 30,000 hospital-acquired infections in 2006, report says.** More than 30,000 hospitalized patients acquired infections while admitted to a Pennsylvania medical center in 2006, according to a new report issued Thursday by the Pennsylvania Health Care Cost Containment Council. The study marks the second time PHC4 issued a hospital-specific report on hospital acquired infections in the state. In 2005, medical centers reported 19,154 patients with hospital-acquired infections. The council said the increase was caused by an expansion of the hospital-acquired infection reporting categories along with “significant strides” made by hospitals in identifying and reporting infections. PHC4 noted that when comparing data from the two most similar data collection time periods – the fourth quarter of 2005 and the fourth quarter of 2006 – the rate of infection dropped from 16.3 infections per 1,000 patients to 15.1 infections per 1,000 patients. Reducing hospital-acquired infections is one of the goals of the Healthcare Improvement Foundation’s Partnership for Patient Care, an initiative created by a group of Philadelphia area-hospitals with funding support from Independence Blue Cross. The foundation’s president said the PHC4 data helps hospitals evaluate and improve their infection prevention and control efforts. “Although the data collected in 2006 was broader than that collected in 2005, the initial pattern for infection rates is trending downward in southeast Pennsylvania and across the state,” she said. The full report, include hospital-specific data, is available on PHC4’s Web site.

Source: <http://www.bizjournals.com/philadelphia/stories/2008/04/07/daily33.html>

27. *April 10, Asbury Park Press* – (New Jersey) **Heightened awareness increases pill distribution near nuclear power plant.** More than 6,800 of the 162,951 people who live or work within ten miles of the Oyster Creek nuclear power plant in Lacey have gotten potassium iodide pills that could protect their thyroids from radiation within the past two months. That is 2,700 more than the number who did so in a series of Ocean County Health Department clinics during spring 2007, according to a department spokesman. He said 2,300 people got them from the Health Department after publication of a February Asbury Park Press article that said only 4,150 people living near the plant had gotten the free pills during the earlier series of clinics. Another 4,791 got them at three recent clinics held by the department. The Long Beach Island Health Department is offering the pills at a clinic Thursday afternoon. The spokesman said in addition to the heightened awareness following the Press story, a message was put out on the Health Alert Network of the department, and information was provided at post offices and supermarkets.

Source:

<http://www.app.com/apps/pbcs.dll/article?AID=/20080410/NEWS02/804100648>

28. *April 9, FOX News* – (National) **Celebrity medical records hacked: are you at risk?** In the wake of a number of cases of the medical information of celebrities being

accessed, the founder and chairwoman of Patient Privacy Rights, a non-profit advocacy group in Austin, Texas, says all medical records are up for sale to large corporations, research facilities, and drug companies. By signing a Health Insurance Portability and Accountability Act (HIPAA) consent form, she said, you not only are giving your doctor and insurance company access to your medical records, but you may be giving them permission to sell your information, as well. “The privacy rule requires health care providers to give patients a notice of privacy practices to provide them with important information on how their health information may be used and disclosed, as well as what their rights are with respect to their information and how the individual can exercise these rights,” says a senior adviser for HIPAA Privacy Outreach, Office for Civil Rights, U.S. Department of Health and Human Services. A senior fellow and health economist at the National Center for Policy Analysis, a non-profit advocacy group that researches public policy, said many drug companies and researchers buy aggregated information so they can figure out which drugs work and which ones do not.

Source: <http://www.foxnews.com/story/0,2933,348988,00.html>

29. *April 9, Associated Press* – (National) **Study: Waning immunity led to ‘06 mumps outbreak.** Most of the college students who got the mumps in a big outbreak in 2006 had received the recommended two vaccine shots, according to a study that raises questions about whether a new vaccine or another booster shot is needed. The outbreak was the biggest in the U.S. since shortly before states began requiring a second shot for youngsters in 1990. Nearly 6,600 people became sick with the mumps, mostly in eight Midwest states, and the hardest-hit group was college students ages 18 to 24. Of those in that group who knew whether they had been vaccinated, 84 percent had had two mumps shots, according to the study by the Centers for Disease Control and Prevention and state health departments. That “two-dose vaccine failure” startled public health experts, who had not expected immunity to wane so soon – if at all. The mumps virus involved was a relatively new strain in the U.S., not the one targeted by the vaccine, although there is evidence from outbreaks elsewhere the shots work well against the new strain. The researchers, reporting in Thursday’s *New England Journal of Medicine*, note the virus likely came from travelers or students from the United Kingdom, where mumps shots are voluntary and there was a much larger mumps outbreak of the same strain. Many countries do not vaccinate against mumps, so future cases brought from overseas are likely.

Source: http://www.usatoday.com/news/health/2008-04-09-mumps-vaccines_N.htm?csp=15

30. *April 9, Reuters* – (National) **WellPoint probing data breach for 130,000 members.** Health insurer WellPoint Inc. is investigating the cause of a breach involving protected health information for about 130,000 members, the company said on Wednesday. The largest U.S. health insurer by membership said it recently discovered data that had become publicly available over the Internet in the past 12 months. The information may have included member ID numbers, possibly including social security numbers, and pharmacy or medical data. A spokeswoman said the company fixed the problems and is notifying members. The problems stemmed from two Internet servers maintained by third-party vendors, the company said. WellPoint said it is investigating the issue

internally and with external consultants.

Source:

http://news.yahoo.com/s/nm/20080409/us_nm/wellpoint_data_dc;_ylt=AhQzWmBZ2OmSZyyYjrLnUfwWIr0F

Government Facilities Sector

31. *April 9, WPXI 11 Pittsburgh* – (Pennsylvania) **Pipe bomb found on Pitt campus.** The bomb squad was called to the University of Pittsburgh campus overnight. A police officer walking his beat around 2:45 a.m. Wednesday when he found a pipe outside the Student Union. The pipe has been determined to be safe. There were no evacuations. Police are continuing their investigation.

Source: <http://www.wpxi.com/news/15832336/detail.html>

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

Emergency Services Sector

32. *April 9, CNN* – (National) **FCC approves emergency alert text-messaging system.** Cell phone users will get text message alerts of emergencies under a new nationwide alert system approved late Wednesday by the Federal Communications Commission, according to an FCC spokesman. An emergency text message would be sent in the event of a widespread disaster, severe weather or child abduction. Under the plan, the FCC will appoint a federal agency to create the messages and pass them on to cell phone companies that choose to participate, an FCC representative said earlier. Once that agency is named, the participating cell phone providers would have 10 months to comply with the new system's requirements. "It is essential that we support and advance new ways to share critical, time-sensitive information with them in times of crisis," the FCC chairman said in a written statement. Earlier, the FCC representative explained how the plan would work. Cell phone companies that voluntarily opt into the system would send text-based alert messages to subscribers in response to three types of events: a disaster that could jeopardize the health and safety of Americans, such as a terrorist attack; imminent or ongoing threats such as hurricanes, tornadoes or earthquakes; child abductions or Amber alerts. T-Mobile, Verizon, Sprint Nextel and AT&T all stated that they would be likely to opt into the alert system if it is passed by the FCC.

Source: <http://www.cnn.com/2008/TECH/04/09/fcc.cell.phone.alert/index.html>

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

Information Technology

33. *April 10, Computer Weekly* – (National) **RSA 2008: spot the warning signs of insider attacks.** Insider attacks on corporate information are highly predictable, but nearly half of companies face losses because they ignore the warning signs, say US researchers. This emerged in follow-up research into attacks revealed in the 2007 E-Crimewatch

survey of 671 firms conducted for the US Secret Service and Microsoft by Carnegie Mellon University's (CMU) Software Engineering Institute's CERT program, and interviews with convicted attackers. A senior member of CMU's Cert team told RSA 2008 delegates that there were both behavioral and technical changes that pointed to a raised risk of an attack on corporate information. Technical changes include the creation of unknown access paths to corporate data, such as back doors, logic bombs, theft of other account holders' identity and privileges, and special relationships with other staff members, she said. Attackers were likely to be highly skilled and develop sophisticated attacks, sometimes planned over many months. Their attacks were more likely close to their employment termination dates, and their impact was likely to be greater.

Source: <http://www.computerweekly.com/Articles/2008/04/10/230233/rsa-2008-spot-the-warning-signs-of-insider-attacks.htm>

34. *April 10, IDG News Service* – (National) **DHS offers first take on Cyber Storm exercise.** With its latest Cyber Storm II exercise now completed, the U.S. Department of Homeland Security said it expects to release an after-action report analyzing the event, and is now beginning planning for Cyber Storm III in 2010. Cyber Storm II was a week-long, cyber-security simulation that included mock attacks on transportation and computer systems. But the exercise brought in many more players from government and other industries: about 2,500 people from the U.S., U.K., Canada, Australia, and New Zealand. DHS's assistant secretary for Cyber Security and Communications described a typical Cyber Storm II scenario, in an interview at the RSA Conference in San Francisco Wednesday: "You have a simulated incident that comes in over the e-mail and it may have only to do with the chemical sector at this point. There's an employee in the chemical sector who's arrested," he said. "He was fired the day before and did something to sabotage the network...so somebody in the chemical sector gets that. 'OK what do I do with that?'" The exercise even simulated the media's response. "You have mock news reports," he said. "It shows up on the Web as a news story. People are reading that and they have to separate out what's the level of hearsay in the news report." By participating in Cyber Storm II, emergency response managers could find out if their plans worked out as expected, and, in particular, if people wound up doing what the planners thought they would do, said a senior information systems manager at the Dow Chemical Company, speaking during a conference panel discussion. Because some of the findings from the exercise are sensitive, the DHS will not discuss specifics until the after-report is issued, and that is not expected to happen until August at the earliest. Source: http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/08/04/10/DHS-offers-first-take-on-Cyber-Storm-exercise_1.html

35. *April 9, Times Online* – (National) **US security chief: cyber-threats 'on par' with 9/11.** Computer-based threats are now as serious as those in the material world, said the Homeland Security secretary today at the RSA Security conference in San Francisco. He said that computer-based attacks had the ability to cripple financial institutions and government networks. "We take threats to the cyber world as seriously as we take threats to the material world," he told the gathering of security industry experts. His remarks came as a report by the British Chambers of Commerce found that 23 per cent

of UK businesses had suffered from an attack by malicious software in the past year – more than twice the number that had been the victim of credit card fraud. He said that the US Government planned to shift its approach to fighting computer-based crime from what he called “a fundamentally backward-looking architecture” – analyzing attacks as they happened and tracing back to their source – to “an early-warning system.” He declined to elaborate on how officials would monitor and flag up threats before they materialized, saying the details were classified, but admitting that the new approach presented significant technical challenges. He said that there were too many openings in government networks through which cyber-criminals were able to inject malicious software, and that one of the first goals of the new system would be to reduce the number of access points from thousands to about 50.

Source: http://technology.timesonline.co.uk/tol/news/tech_and_web/article3712868.ece

36. *April 9, Network World* – (National) **Experts hack power grid in no time.** Cracking a power company network and gaining access that could shut down the grid is simple, a security expert told an RSA audience, and he has done so in less than a day. The expert, a penetration-testing consultant, says he and a team of other experts took a day to set up attack tools they needed then launched their attack, which paired social engineering with corrupting browsers on a power company’s desktops. By the end of a full day of the attack, they had taken over several machines, giving the team the ability to hack into the control network overseeing power production and distribution. He says he and his team were hired by the power company, which he would not name, to test the security of its network and the power grid it oversees. He would not say when the test was done, but referred to the timeframe as “now.” The company called off the test after the team took over the machines. The problem is pervasive across the power industry, he says, because of how power company networks evolved. Initially their supervisory, control and data acquisition (SCADA) networks were built as closed systems, but over time intranets and Internet access have been added to the SCADA networks. Individual desktops have Internet access and access to business servers as well as the SCADA network, making the control systems subject to Internet threats. “These networks aren’t enclosed anymore. They’ve been open for more than a decade,” he says.

Source: <http://www.networkworld.com/news/2008/040908-rsa-hack-power-grid.html>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at 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

37. *April 10, ars technica* – (International) **Researchers map Internet black holes.** A University of Washington research project that tracks down Internet black holes – places where packets vanish – has created a [live map](#) system which shows the locations

of these anomalies, updating itself every fifteen minutes. The monitoring system, called Hubble, uses approximately 100 PlanetLab sites around the world to ping various IP prefixes in search of black holes. It uses a hybrid monitoring approach which conducts passive analysis on Border Gateway Protocol (BGP) feeds and launches targeted active probes when it detects potential problem areas. The researchers say that Hubble can detect 85 percent of all Internet “reachability” problems. In three weeks of collected data, the researchers found over 31,000 “reachability” problems, 10 percent of which lasted for over a day. Most of the network problems detected by Hubble are partial “reachability” failures, which means that sites can be accessed from some locations but not others. The Hubble map system lets users click various points to see which locations have access to a given point during a partial “reachability” failure. “There’s an assumption that if you have a working Internet connection then you have access to the entire Internet. We found that’s not the case,” said a UW doctoral student. According to the researchers, ongoing data collection could help network operators identify and resolve problems faster and could also potentially be used to create network detour systems that automatically route traffic around black holes for applications that require uninterrupted service. Researchers hope that more study will provide solutions to routing and “reachability” problems, making it possible to improve Internet robustness. Source: <http://arstechnica.com/news.ars/post/20080410-researchers-map-internet-black-holes.html>

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

Commercial Facilities Sector

38. *April 10, Associated Press* – (International) **China ‘uncovers Olympic terror plot.’** China said Thursday it had uncovered a criminal ring planning to kidnap athletes, foreign journalists and other visitors at the Beijing Olympic Games. Thirty-five members of a ring based in the restive western Xinjiang region were arrested, a Ministry of Public Security spokesman told a news conference. He added that police had also confiscated almost 22 pounds of explosives and eight sticks of dynamite and “jihadist” literature in the latest raids in Urumqi, the capital of Xinjiang. The arrests took place between March 26 and April 6, he said. The official also provided further details on a second group arrested in January, alleging they had been manufacturing explosives and were plotting to attack hotels, government offices and military targets in Shanghai, Beijing and other cities. He said the gang had been acting on orders from a radical Islamic Xinjiang independence group, East Turkestan Islamic Movement. Since the September 11, 2001 terror hijackings, China has tried to portray the simmering separatist rebellion in Xinjiang as being fueled by terrorist organizations in Central Asia and the Middle East. But evidence made public has been scarce. Western embassies asked Beijing for more information after authorities said they broke up an attempt to hijack a plane in western China last month but so far no evidence has been provided, diplomats have said. Source: <http://www.cnn.com/2008/WORLD/asiapcf/04/10/china.plot.ap/index.html>

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

National Monuments & Icons Sector

Nothing to Report

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

Dams Sector

39. *April 9, Associated Press* – (Louisiana) **2 low levees breached; Gov asks disaster declaration for one.** Waves have eaten a chunk five feet deep and ten to 12 feet wide in a six-foot wetlands protection levee, and Terrebonne Parish, Louisiana, levee officials have set aside \$35,000 to plug the hole with rocks before the winds change and waters rise higher. The decision came as Louisiana's governor asked the U.S. Agriculture Department secretary to declare Pointe Coupee Parish a federal disaster area because of a "potato levee" breach in the Morganza Spillway. The breach will keep some farmers from planting cotton and soybeans, and others have lost wheat and crawfish to floods and heavy rains, a spokeswoman for the governor told the secretary. The governor asked the secretary to declare the parish a disaster area, along with six surrounding parishes: Avoyelles, Concordia, Iberville, St. Landry, West Baton Rouge, and West Feliciana. The 18,000-foot Montegut Marsh Management levee is not a hurricane-protection levee, officials said, but protects lower-Terrebonne communities by controlling saltwater intrusion into the Pointe-aux-Chenes State Wildlife Management Area. Wildlife and Fisheries officials first noticed the breach a month ago but could not get money to fix it immediately and came to the Terrebonne Levee and Conservation District for help, said the executive director of the district.

Source: <http://www.nola.com/newsflash/index.ssf?/base/news-38/1207750449186970.xml&storylist=louisiana>

40. *April 9, WIBW 13 Topeka* – (Kansas) **Reno County still trying to strengthen levees.** Officials in Reno County are looking for ways to strengthen a nine mile stretch of levee that failed in torrential spring rains last year. Thousands of acres of land were swamped when the Arkansas River breached its levee in five places last spring. Whole sections, one as large as 600 feet in length, were washed out. In just the last few weeks, final repairs have been made to some of the levees. But authorities worry they may not hold against another major flood. Therefore, plans are underway to make the levees taller and stronger in certain places. Homeowners with properties next to the river recently approved a \$175,000 bond, which will pay for adding 12 inches of dirt to the top of the levee system. In areas where the Arkansas River bends, the waters eat away at the levee. A board member of the levee district says he is working with the U.S. Army Corps of Engineers to retrofit those particularly weak points in the levee with rock and concrete. The board member also hopes to begin strengthening the sides of the levee in places where the river cuts into it as soon as he can get approval from the Corps.

Source: <http://www.wibw.com/kakeheadlines/headlines/17449499.html>

41. *April 9, Carroll County Comet* – (Indiana) **NIPSCO submits dam analysis.** Northern Indiana Public Service Company (NIPSCO), which operates Norway and Oakdale dams,

submitted a dam analysis to the Federal Energy Regulatory Commission Friday. FERC requested the report after local flood victims questioned whether the dams could have been operated to mitigate downstream damage during January floods. According to information supplied by NIPSCO, the study was prepared to “evaluate possible changes in the way the dams operate in order to eliminate or reduce downstream flooding that occurs under the current run-of-the river operating procedures for floods ranging from a ten-year flood to a 500-year flood.”

Source: http://www.carrollcountymet.com/news/2008/0409/Front_Page/005.html

42. *April 9, Carroll County News* – (Arkansas) **112-year-old Black Bass Lake Dam may put city ‘between a rock and a hard place.’** The City of Eureka Springs, Arkansas, may find itself “between a rock and a hard place” concerning Black Bass Lake Dam, as it will have to ponder what action to take following a visit by a Carroll County judge and county, city, and state officials Friday. The judge told the group, “Last week the FEMA people were here, and their comment was, ‘Not if, but when will something happen.’” In 2004, Eureka police officers raised the alarm that the 112-year-old masonry dam was leaking severely, and the department alerted Public Works. The city funded repair work, and holes were drilled through the top deck of the dam, and voids were filled within the dam with pumpable pressure grout. “We reduced the seeping considerably,” said a representative of Tracy Consulting Engineers. “We low-pressure cement-grouted the worst areas.” He said there is no way to assess how long the repair would last, and what was done was a “temporary fix.” There is still some leakage at the dam now. The dam is not a “permitted” dam, meaning the state does not inspect it for safety. In 1981, on an engineering recommendation, the lake level was drawn down so that flow volume and surface area (under normal conditions) were not a hazard and were then below the levels requiring state inspection. But no one foresaw a rainfall of seven inches in a 24-hour period that has made Carroll one of 44 counties currently declared disaster areas by the governor.

Source: <http://www.eurekaspringstimesecho.com/articles/2008/04/09/news/mw1.txt>

43. *April 9, WKYT 27 Lexington* – (Kentucky) **Wolf Creek Dam needs major repairs, magazine says.** Southern Kentucky’s Wolf Creek Dam that holds back Lake Cumberland has landed on an ominous list. Popular Mechanic magazine lists the huge dam as one of the top ten pieces of U.S. infrastructure that must be fixed now. Engineers say the limestone foundation is dissolving at an alarming rate which weakens the structure and threatens communities downstream. The earliest possible completion date for repairs to the dam is 2012.

Source: <http://www.wkyt.com/wymtnews/headlines/17422389.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 NICCRReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Removal from Distribution List:	Send mail to NICCRReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 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 or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

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