



Department of Homeland Security Daily Open Source Infrastructure Report for 23 May 2008

Current Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

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

- According to Bloomberg, Swedish bomb technicians found no unusual objects in a nuclear reactor they investigated after police arrested two men yesterday on suspicion of sabotage. The plant was turned off Wednesday and was searched by police Thursday. (See item [3](#))
- The Day reports that several hundred thousand People's United Bank customers in Connecticut were hit by a data breach in February when the Bank of New York Mellon lost an unencrypted backup tape provided by People's Bank. The state's attorney general's office said the tape included bank account information, Social Security numbers and other data about depositors and investors tied to the bank, and involved about 4.5 million accounts. (See item [10](#))

DHS Daily Open Source Infrastructure Report Fast Jump

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

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

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

Federal and State: [Government Facilities](#); [Emergency Services](#); [National Monuments and Icons](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: **Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *May 22, Bloomberg* – (International) **Oil declines more than \$1 a barrel on signs rally unjustified.** Crude oil fell more than \$1 a barrel on signs that the 16 percent run-up in prices this month is not justified by stockpiles and demand. Consumption averaged 20.3 million barrels a day in the past four weeks, down 1.3 percent from a year earlier, the U.S. Energy Department said. Crude oil for July delivery fell \$1.47 to \$131.70 a barrel at 10:38 a.m. on the New York Mercantile Exchange after reaching a record \$135.09.

Source:

<http://www.bloomberg.com/apps/news?pid=20601072&sid=aavx1azJoxKw&refer=energy>

2. *May 21, Reuters* – (California) **Power system to meet California summer demand-study.** California should have adequate power supplies this summer, even if the state experiences warmer-than-normal temperatures, the California Energy Commission said in a summer outlook Tuesday. In the forecast, the Commission said ample resources should be available to meet peak loads and operating reserves will be sufficient even with a very warm summer. The Commission, however, urged consumers to continue conserving electricity on hot afternoons. The outlook showed reserve margins, or the level of electricity supplies above demand, are about 22 percent for average weather conditions and 14 percent under hotter-than-normal weather. California, however, is divided into regions north and south of Path 26, a transmission line area that frequently has constraints during periods of high electricity demand. Under hotter-than-normal temperatures, the Commission said supplies could be tight in southern California with reserve margins dipping below the 15 percent to 17 percent target.

Source:

<http://www.reuters.com/article/marketsNews/idUSN2140775320080521?pageNumber=1&virtualBrandChannel=0>

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

Chemical Industry Sector

Nothing to report

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

Nuclear Reactors, Materials, and Waste Sector

3. *May 22, Bloomberg* – (International) **Swedish nuclear plant search finds no suspect objects.** Swedish bomb technicians found no unusual objects in a nuclear reactor they investigated after police arrested two men yesterday on suspicion of sabotage. Reactor 1, adjacent to the unit where the men worked, was turned off Wednesday and will be searched by police Thursday, said a spokesman for plant operator OKG AB. The generator is scheduled to resume service on May 24, German utility E.ON AG, which owns a majority of OKG, said Thursday. The two contract welders, who were detained after one of them was caught in a security check Wednesday morning when traces of explosives were found on a carrying bag, were released Thursday, Ekot radio reported. While the suspicions against the men remain, there was no need to keep them in custody any longer, said a Kalmar county prosecutor. “The search of reactor 1 is a pure safety measure, as we cannot be 100 percent sure that the men didn’t have access to space shared with unit 2,” said the OKG AB spokesman.

Source:

<http://www.bloomberg.com/apps/news?pid=20601072&sid=a6OfhK0e2EyE&refer=energy>

4. *May 22, Toledo Blade* – (Michigan) **Fermi 1 fire emitted no radiation.** The U.S. Nuclear Regulatory Commission (NRC) said Wednesday it found no evidence of external radiation from a small fire that broke out about 2:00 p.m. Tuesday inside the decommissioned Fermi 1 nuclear plant. The fire began in the basement when residual liquid sodium made contact with air. That occurred as a pipe holding the material was moved by workers outside the plant who were doing an inspection with remote equipment, said a DTE Energy spokesman. An NRC spokeswoman said the fire was presumed radioactive because liquid sodium was used to cool the plant's reactor. External monitoring continues, she said. The decommissioning project has been temporarily suspended, pending an evaluation.
Source: <http://toledoblade.com/apps/pbcs.dll/article?AID=/20080522/NEWS07/805220372/-1/NEWS>
5. *May 21, San Luis Obispo Tribune* – (California) **Crane mishap damages weather tower at Diablo Canyon.** A mishap with a mobile crane early Wednesday damaged a meteorological tower at Diablo Canyon nuclear power plant. The crane was being moved between 7:00 and 8:00 a.m. when it hit a guy wire holding the 250-foot tower. The tower is still standing, but it is damaged, and plant workers will do a structural assessment to determine the extent of the damage, said a plant spokesman. As a safety precaution, part of a parking lot near the plant's cooling water intake cove is barricaded off, and several buildings used for training are not being used.
Source: <http://www.sanluisobispo.com/breakingnews/story/366583.html>
6. *May 21, Associated Press* – (Texas) **Dallas company gets state license to bury nuclear waste at west Texas site.** State environmental regulators on Wednesday gave approval for a Dallas-based company to dispose of Cold War-era radioactive waste at a site in west Texas where it is now being stored. Waste Control Specialists worked for four years to secure the license, which was approved by a 2-1 vote of the Texas Commission on Environmental Quality in Austin. The company still has about six months of construction before it can begin burying the 3,776 canisters of the uranium byproduct waste in far western Andrews County near the New Mexico border. A Sierra Club activist said an appeal of the commission's vote is probable.
Source: http://www.dallasnews.com/sharedcontent/dws/news/texasouthwest/stories/052208dnte_xnukewaste.1f38339.html

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

Defense Industrial Base Sector

7. *May 22, Navy Times* – (Mississippi) **2 injured in Mississippi T-45C crash.** A Navy T-45C Goshawk assigned to Training Air Wing 1 crashed Tuesday night just south of a runway at Naval Air Station Meridian, Mississippi, while on a routine training mission, according to a statement released Wednesday by Naval Air Forces. An investigation is underway to determine the crash's cause.

Source: http://www.navytimes.com/news/2008/05/navy_t45crash_052108w/

8. *May 22, Network World* – (National) **Feds encrypt 800,000 laptops; 1.2 million to go.** U.S. government agencies are scrambling to plug one of their biggest security holes: sensitive information – names, addresses and Social Security numbers, for example – stored on laptops, handhelds and thumb drives. In the last year, agencies have purchased 800,000 licenses for encryption software through the federal Data at Rest (DAR) Encryption program, which is run jointly by the General Services Administration and the U.S. Department of Defense. The government’s fast adoption rate of encryption software comes after numerous headline-grabbing security breaches. Laptop encryption has also been on the rise among corporations, including the likes of EMC and IBM. This year alone, laptops with personally identifiable information have been stolen from Bolling Air Force Base, a Marine Corps base in Okinawa, Japan and the National Institutes of Health in Bethesda, Maryland. In all of these cases, data that was not encrypted on these laptops could have been used by thieves for identity theft, according to a list of known security breaches compiled by the Privacy Rights Web site. While sales on the DAR Encryption program are stronger than anticipated, federal officials admit they have not secured all of their laptops, handhelds and removable drives yet. Source: <http://www.networkworld.com/news/2008/052008fedlaptops.html?page=1>

9. *May 22, KOAA 530 Colorado Springs* – (Colorado) **Pueblo Chemical Depot builds new plant to neutralize chemical weapons.** East of Pueblo, construction is underway on a new multi-billion dollar processing plant at the Pueblo Chemical Depot. When completed, the U.S. Department of Defense (DOD) will use it to destroy 2,600 tons of chemical weapons currently stored in igloos at the depot. Workers are building several new buildings which collectively will be known as the Pueblo Chemical Agent Destruction Pilot Plant. It is a \$3.5 billion project. The primary function of the plant will be to neutralize the mustard agent stored at the depot since the 1940s. The plant is scheduled to be completed by 2013 and open for operations in 2015. The DOD is under a federal deadline to destroy the munitions by the end of 2017. By 2023, the plant is scheduled to be taken apart. Source: http://www.koaa.com/aaa_top_stories/x1331637897

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

Banking and Finance Sector

10. *May 22, The Day* – (Connecticut) **People’s Bank customers at risk from data breach.** Several hundred thousand People’s United Bank customers in Connecticut have been hit by a data breach that potentially exposed their personal information, a state Attorney General said Wednesday. He said the Bank of New York Mellon lost an unencrypted backup tape provided by Bridgeport-based People’s Bank, resulting in the data breach involving about 4.5 million accounts. The tape included bank account information, Social Security numbers and other data about depositors and investors tied to the bank, he said. The official was particularly concerned with the amount of time that elapsed between the discovery of the data breach and the reporting of it. Bank of New York lost the information in February but did not start informing consumers until six weeks ago,

the official said. He said the Bank of New York Mellon on February 27 gave an unencrypted backup tape as well as nine other tapes to a storage firm, Archive Systems Inc. of Fairfield, New Jersey, which was assigned to store the information. But when a storage company vehicle arrived at the storage facility, one of the tapes could not be found. According to a letter from the official to the Bank of New York, a lock on the truck was broken, and the truck had been left unattended several times. People's Bank has 10 locations in southeastern Connecticut and more than 150 locations statewide. Source: <http://www.theday.com/re.aspx?re=1a830cf7-5c18-476e-84b5-0d8b0162ff00>

11. *May 22, Washington Post* – (District of Columbia) **Banker admits to role in tax office scam.** A former Bank of America manager pleaded guilty yesterday to participating in a massive embezzlement at the District of Columbia tax office, admitting that he deposited nearly \$18 million in fraudulent checks and helped distribute the stolen money to others in the scam. Authorities say up to \$50 million in property tax money was stolen in the form of fraudulent refund checks in a scam allegedly orchestrated by a former tax office manager, who is in jail awaiting trial. She has pleaded not guilty. The theft was the biggest municipal fraud in memory in the Washington area. Only a small fraction of the money has been recovered.

Source: <http://www.washingtonpost.com/wp-dyn/content/story/2008/05/21/ST2008052102629.html>

12. *May 21, Reuters* – (Idaho) **Five indicted in \$20 million Idaho mortgage scam.** An Idaho bank officer and four others accused of masterminding a mortgage scam were indicted in Boise on Wednesday on charges of defrauding an Idaho bank of \$20 million, according to federal prosecutors. Authorities say the accused, including two building contractors, a mortgage broker and a Realtor, all from the Boise, Idaho area, provided false financial data and fraudulently fronted applicants -- known as straw buyers -- in attempt to obtain 49 house loans. The FBI has linked a jump in mortgage fraud to "an ideal climate" created by the slump in the U.S. housing market.

Source: <http://www.reuters.com/article/domesticNews/idUSN2142808620080522>

13. *May 21, U.S. World News* – (National) **Warning: Chinese earthquake scam reported.** The FBI is warning consumers to be on the lookout for E-mails purportedly soliciting funds to support the victims of the recent earthquake in China. "Some of the Chinese earthquake scam messages claim to be offering free vacation trips to the largest donors and even use fake logos of legitimate online pay services to fool people," the FBI said in a release. Similar fraudulent efforts followed other recent tragedies, such as 9/11, Hurricane Katrina, and the shootings at Virginia Tech, the FBI said. Criminals apparently use such events to prey upon the sympathy of individuals.

Source:

http://www.banktech.com/aml/showArticle.jhtml?articleID=207800150&cid=RSSfeed_BankTech_News

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

Transportation Sector

14. *May 22, New York Times* – (National) **F.A.A. bans antismoking drug, citing side effects.** The Federal Aviation Administration (FAA) said Wednesday it would no longer permit pilots or air traffic controllers to use the smoking cessation drug Chantix, citing potential side effects that could pose a threat to the safe operation of aircraft. The Food and Drug Administration issued a public health advisory in February, saying that some users had developed a variety of serious psychiatric symptoms, and some had committed suicide. An FAA spokeswoman said the agency had approved the drug's use for airline pilots and flight controllers last year, but was notifying 150 pilots and 30 air traffic controllers known to be using it that the drug was no longer acceptable and should be discontinued. The FAA was also planning to notify associations representing both commercial and private pilots that Chantix was no longer permitted, the official said. Source: <http://www.nytimes.com/2008/05/22/business/22drug.html?ref=health>

15. *May 21, KSDK 5 St. Louis* – (Missouri) **Lambert Airport reports another security incident.** For the third time in as many weeks, a security incident has occurred at Lambert-St. Louis, Missouri, International Airport. The latest incident happened last Saturday night. An airport spokesman said a woman reentered the exit of a concourse. It is unknown how the woman was able to get past security, but a sweep of the concourse found the woman and a subsequent search turned up nothing suspicious. Source: http://www.ksdk.com/news/news_article.aspx?storyid=146681

16. *May 21, Daily Pilot* – (California) **Knife found on JWA plane; TSA points to employees.** Nearly 200 passengers boarding a flight from John Wayne Airport, Orange County, California, to Phoenix, Arizona, on Wednesday had to disembark after a passenger found a knife aboard the plane, airport officials said. A passenger aboard the 10 a.m. U.S. Airways flight to Phoenix found a 3-inch pocket knife on the floor of the plane and turned it over to the flight crew, an airport spokeswoman said. The 190 passengers went through security screening before boarding again, she said. No passengers were detained. Transportation Security Administration officials are focusing their investigation on pre-flight crews. A TSA spokesman said it is unlikely a passenger got the knife through security. An airline employee or plane staffer most likely dropped it between flights, he said. Source: <http://www.dailypilot.com/articles/2008/05/22/publicsafety/dpt-jwaknife052208.txt>

17. *May 21, Star Tribune* – (Minnesota) **Minnesota's 'worst' bridge to be replaced.** The worst bridge in Minnesota is about to be replaced. The "Iron Bridge" over the Cannon River on the outskirts of Northfield has an extraordinarily rare sufficiency rating of 0.00. It has long hovered on the edge of closure. "We are monitoring it all the time," a Dakota County design engineer said Wednesday about the bridge, which is No. 1 on the state's list of deficient bridges. "If it gets any worse at all, we'd strongly consider closing it." One challenge in replacing the bridge is that it is located near Carleton College's Cowling Arboretum. It has taken a long time for the college, the state, Dakota County and Waterford Township to work out a deal to cross that land with a new bridge while retaining the old one as a link in a future state trail. That deal was announced early this week. The new bridge, at about 300 feet, will be much longer than the old one and will

be several hundred feet upstream. It is expected to cost about \$1.5 million, and construction is to begin as soon as this fall. The bridge is a shortcut between the two major arteries -- Hwys. 47 and 19 -- leading eastward out of the northern part of town. About 400 cars cross it per day, according to Dakota County officials.

Source: http://www.startribune.com/local/south/19155759.html?location_refer=Books

18. *May 21, Reuters* – (Alaska) **Alaska probes oil spill at Conoco’s Alpine field.** Alaska State regulators are investigating a small oil pipeline leak at ConocoPhillips’ Alpine field last weekend that was caused by corrosion on the line. The incident, which resulted in a spill of 170 gallons of oil, comes two years after severe pipeline corrosion at BP’s Prudhoe Bay oil field led to the biggest spill on record on Alaska’s North Slope. The Alaska Department of Environmental Conservation said the leak at Conoco’s Alpine field came out of a pinhole-sized hole in a low pressure pipeline, and was a surprise because the field is relatively new. A coordinator for the Department of Environmental Conservation said one theory about the corrosion is that it was caused by water settling in low parts of the line, as the pinhole was detected in one of the low spots. ConocoPhillips has placed a sleeve on the affected section of pipeline, and production from the field has not been significantly affected, he said.

Source: <http://www.reuters.com/article/marketsNews/idUSN2149945620080521>

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

Postal and Shipping Sector

19. *May 21, Southwest Iowa News* – (Iowa) **‘Suspicious’ package considered non-hazardous after Hazmat team summoned.** An unidentified substance in a package that caused Ames, Iowa, postal officials to call in the Des Moines Hazardous Materials Unit to investigate has been determined to be non-hazardous, according to a postal inspector. The package, described by the official as a bubble-wrapped envelope carried by the post office, apparently came under suspicion when workers at the post office saw that the item was stained. The lobby of the office remained open throughout the episode, but the rear shipping area of the post office was shut down as investigators worked to determine what the substance was. Employees who had been exposed to the package were kept on hand until the nature of the substance in the package was determined. An ongoing investigation between the post office and the Ames Police Department will continue to determine the origin of the package.

Source:

http://www.southwestiowanews.com/site/news.cfm?newsid=19707563&BRD=2703&PAG=461&dept_id=627131&rfi=6

20. *May 20, San Diego Union-Tribune* – (California) **Lakeside bomb scare a false alarm.** A sheriff’s bomb squad found nothing sinister Tuesday afternoon when they investigated a suspicious object found in a Federal Express drop-box in front of the Lakeside, California Post Office. Within an hour, the bomb experts arrived and determined the object was not an explosive.

Source:

http://weblog.signonsandiego.com/news/breaking/2008/05/lakeside_bomb_scare_a_fals

[e_al.html](#)

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

Agriculture and Food Sector

21. *May 22, USAgNet* – (National) **House votes to override President’s Farm Bill veto.** President Bush vetoed the long-embattled 2007 farm bill Wednesday, saying it provides subsidies for farmers at a time of record crop prices, increases farm spending by \$20 billion, and uses “budget gimmicks to hide much of that increase.” But within hours, in a show of bipartisan defiance, the House overwhelmingly overrode his veto of the nearly \$300-billion bill by a vote of 316 to 108. But an embarrassing legislative snafu may well nullify the House’s veto override and trigger a string of new votes that could reopen the farm bill for consideration. The mix-up occurred in the House, which sent the White House the final version of the bill minus one 34-page section. Because the White House did not receive the entire farm bill, House leaders were left wondering whether Bush’s veto, and their override vote, was legitimate. The Associated Press reported late Wednesday that the House may have to vote to reapprove the bill in an expedited manner today, send it back to Bush for a new veto, then hold another override vote.
Source: <http://www.usagnet.com/story-national.php?Id=1220&yr=2008>
22. *May 21, CattleNetwork* – (Oregon) **FSIS issues alert for beef products due to possible E. coli contamination.** The U.S. Department of Agriculture’s Food Safety and Inspection Service (FSIS) is issuing a public health alert for approximately 808 pounds of ground beef products produced at Tyson Fresh Meats, Inc. that may be contaminated with E. coli O157:H7. Tyson Fresh Meats, Inc. sold chubs of 85 percent lean, 15 percent fat coarse ground beef to Sherm’s Food-4-Less retail establishment in Medford, Oregon, who then processed this ground beef into various sized packages of ground beef products and sold to consumers between May 7 and May 19. FSIS is issuing a public health alert rather than a recall because FSIS has confirmed that none of the affected products remain available for sale at this retail establishment.
Source: <http://www.cattlenetwork.com/Content.asp?ContentID=223527>

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

Water Sector

23. *May 22, USA TODAY* – (National) **Proposed change to water law riles landowners.** A proposal backed by environmentalists to change one word in the Clean Water Act and subject tens of millions more acres of land to new federal oversight has angered ranchers and farmers. A lawyer for the National Wildlife Federation says the law must be revised to protect not only the water on the lands at issue but the waters they flow into. He says the waters and wetlands now outside the scope of the law “provide incredible functions to the health of all watersheds” and are valuable as aquatic habitats, sources of drinking water, and flood prevention. The Clean Water Act of 1972 makes it illegal to pollute “navigable” waters. Over the decades, disputes arose over the government’s expanding definition of “navigable,” and some landowners complained that the word was being

interpreted too broadly. Two Supreme Court decisions in 2001 and 2006 came down on the side of landowners, ruling that ponds at the bottom of a gravel pit and a marsh miles from any lake or river were not navigable and thus not subject to the act. The new definition would place under federal oversight all water subject to the ocean tides as well as “lakes, rivers, streams, mudflats, sandflats, wetlands, sloughs, prairie potholes, wet meadows, playa lakes, natural ponds and all impoundments,” also known as man-made reservoirs. The Illinois Farm Bureau says the language would cover an additional 55 million acres. The president of the Iowa Corn Growers Association says the bill would place an unreasonable burden on people who are not polluting but just raising crops and livestock and using water to do it.

Source: http://www.usatoday.com/news/nation/environment/2008-05-21-water-law_N.htm

24. *May 21, Seattle Post-Intelligencer* – (Northwest) **Ban on cruise ship sewage discharges near shellfish beds.** The NorthWest CruiseShip Association, an organization representing the cruise ships traveling to and from the Port of Seattle, has agreed to prohibit discharges of treated sewage within a half-mile of shellfish beds as recommended by the state Health Department. Dumping of raw sewage within Puget Sound and the Strait of Juan de Fuca south of the international boundary with Canada is prohibited, under a voluntary arrangement struck in 2004 and updated annually by its signers – the cruise association, the Port of Seattle, and the state Ecology Department. The average Alaska-bound cruise ship generates about 28,000 gallons of sewage sludge during the seven-day jaunt from Seattle, according to port staff. The port is studying whether it would be feasible and advisable to truck the sewage to a treatment plant rather than dumping it in the ocean. The cruise lines have also recently agreed to stop discharging treated sewage when gastroenteritis cases exceed two percent of passengers or crew for this season.

Source: http://seattlepi.nwsourc.com/local/363993_cruise22.html

25. *May 21, East Valley Tribune* – (Arizona) **EPA cuts off use of faulty Scottsdale well.** The well that led to two water contamination scares in October and January will not serve Arizona American Water Co. customers for at least a year while a long-term remedy is developed, the U.S. Environmental Protection Agency (EPA) said Wednesday. Treated water from that well at the Miller Road Treatment Facility in Scottsdale will continue to be dumped into the Arizona Canal. Meanwhile, the three companies that operate the facility – Motorola, Siemens Corp., and GlaxoSmith Kline – will develop long-term solutions to be presented to the EPA in the fall. The companies were fined \$500,000 on Monday by the EPA for the system failures. The companies are responsible for polluting groundwater under a vast swath of Scottsdale with TCE, beginning in the mid-1950s. The chemical was generally used as an industrial solvent.

Source: <http://www.eastvalleytribune.com/story/116853>

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

Public Health and Healthcare Sector

26. *May 22, Agence France-Presse* – (International) **Bangladesh reports first human case**

of bird flu. Bangladesh reported its first confirmed case of human bird flu on Thursday, but said the 16-month-old victim had now recovered from the virus. The baby boy from a Dhaka slum was diagnosed with the H5N1 strain of the disease in January, but this was only confirmed by a U.S. laboratory this week, the government said. A senior government official, who works for the livestock ministry and is coordinating Bangladesh's battle against bird flu, said that the virus was "very much under control." "We're destroying the birds and eggs as soon as we have any report of bird flu at any farm in the country," he said.

Source: <http://afp.google.com/article/ALeqM5g-4Jkb3IXeSPaQ5FgaAB0Uh8Zf1w>

Government Facilities Sector

27. *May 22, Hampton Roads Daily Press* – (Virginia) **Courthouses evacuated after bomb threats.** Two Hampton courthouses were evacuated Wednesday morning – for the second time this week – following bomb threats at the buildings. Someone called the city's 911 center, making threats to both Hampton General District Court and Juvenile and Domestic Relations District Court, a Hampton police spokeswoman said. Police evacuated the courthouses at 9:40 a.m. Firefighters and bomb sniffing dogs from the Hampton police, the Virginia State Police, and the Coast Guard helped search both buildings, as people who had been in court waited outside. The buildings were reopened at 11:37 a.m.

Source: http://www.dailypress.com/news/local/hampton/dp-local_bombthreats_0522may22,0,2096334.story

28. *May 21, KOMO 1000 Seattle* – (Washington) **Officials investigate courthouse security breach.** Officials at the King County Superior Courthouse are investigating the circumstances surrounding a security breach on Tuesday in which a gun slipped through a security check point at the courthouse. The screener did not follow procedures which require employees to stop everything when a gun is identified. At 8:40 Tuesday morning at one of the two entrances to the courthouse, a security screener saw what she thought was a gun inside a bag on her monitor, officials said. By the time the sheriff's deputy, who was standing just a few feet away, was told, the gun and its owner were long gone. The screener never got a good look at the real owner, so police do not have a description. No one informed him of the situation until three and a half hours later. The gun and its owner have yet to be found. The presiding judge said inappropriate actions taken by one or more employees allowed the breach to happen.

Source: <http://www.komoradio.com/news/19160094.html>

29. *May 21, Surprise Today* – (Arizona) **Third bomb-like device detonated at Dysart school.** A third bomb-like device has been detonated on the campus of a high school in the Dysart Unified School System, north of Phoenix, Arizona, in less than a month. On Tuesday, May 20, a small homemade incendiary device was brought into Dysart High School and ignited in the cafeteria. The incident created a disturbance and was extinguished by school officials. On April 23 and May 1, chemical bombs were detonated at Willow Canyon High School and Valley Vista High School. On Tuesday,

the school's El Mirage Police Resource Officer was notified, and he took possession of the remains of the device as evidence which he impounded for scientific analysis. An El Mirage detective was notified and assisted in the investigation. The contents of the device will be submitted for scientific analysis at the Department of Public Safety Crime Lab. The resulting investigation revealed that two Dysart High School juniors were responsible for the incident. The students were identified during the investigation and were interviewed Wednesday morning. Both students were arrested and made statements regarding the incident. Both admitted that they found plans for the device on the Internet.

Source:

http://www.yourwestvalley.com/news/school_2632__article.html/device_high.html

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

Emergency Services Sector

30. *May 22, Green Bay Press Gazette* – (Wisconsin) **Port drill puts security, safety plans to the test.** In a full scale exercise Wednesday, 200 people and 35 agencies practiced responding to a situation which simulated a bio-chemical terror plot at Green Bay's port. The drill, funded through a Homeland Security grant in 2007 to Green Bay's port, gave participants a chance to practice, assess, and improve the Lake Michigan Area Maritime Security Plan. The terrorism scenario included multifaceted security and a concern about hazardous materials. "Victims" who had chemical skin irritations were taken to a mobile decontamination unit at the Metro Boat Launch area and then to nearby hospitals for further "treatment." A science officer, meanwhile, tried to determine the type of chemical involved in the drill.

Source:

<http://www.greenbaypressgazette.com/apps/pbcs.dll/article?AID=/20080522/GPG0101/805220481/1978/GPGbusiness>

31. *May 21, Associated Press* – (National) **Border agents won't slow hurricane evacuations.** The U.S. Homeland Security Department secretary clarified that federal border agents would not impede a hurricane evacuation from south Texas by checking fleeing residents' documents, diverting from plans confirmed by Border Patrol officials in the state only days earlier. Texas officials reacted with concern when patrol officials along the Texas-Mexico line said last week that checkpoints 75 miles north of the border would remain in operation during a hurricane evacuation. Officials also had said agents would make checks at evacuation hubs where fleeing residents lacking transportation would board buses. Local emergency management officials feared the checkpoints could become bottlenecks for traffic fleeing the coast and the low-lying Rio Grande Valley, and could dissuade illegal immigrants and legal residents with undocumented family members from heading to safety.

Source:

<http://ap.google.com/article/ALeqM5iFR5DqnuIozOjlXQj2lm7rVELoUgD90QAKQOO>

32. *May 21, Press-Enterprise* – (California) **November drill to tackle 'The Big One.'** A magnitude 7.8 earthquake will erupt along the San Andreas fault at the Salton Sea and

grind its way through the Coachella Valley toward San Bernardino and beyond later this year in the state's biggest-ever drill to test emergency crews. The region's best-known seismologist said Wednesday that another goal of the November 13 drill is to get residents and businesses thinking now about how to prepare for a quake that could kill as many as 1,800 people in southern California. The scenario features a quake nearly as strong as the recent quake in China. Details will be available at www.ShakeOut.org.

Source:

http://www.pe.com/localnews/inland/stories/PE_News_Local_D_quake22.4034d04.htm

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

Information Technology

33. *May 22, BetaNews* – (National) **iCal bugs can lead to DoS and code execution attacks.** Researchers with Core Security have found three vulnerabilities in Mac OS X's calendaring application that could create havoc for users. The most serious vulnerability deals with a memory corruption issue that is triggered by the execution of a specially-crafted .ics file. At the heart of it is a resource liberation bug which is triggered through the file, thus allowing code execution. A user could lose control of his or her Mac through this bug, the firm warned. While it appears the bug needs to be exploited with some intervention from the end-user, Core said it may be exploitable without as well. Both of the remaining flaws deal with denial of service issues, where repeated crashes prevent use of the iCal application. As with the previous bug, a specially-crafted .ics file is launched, which then takes advantage of a null-pointer dereference bug in the software. Core could not find any evidence that this issue could also result in code execution. "Exploitation of these vulnerabilities in a client-side attack scenario is possible with user assistance by opening or clicking on specially crafted .ics file send over email or hosted on a malicious web server; or without direct user assistance if a would-be attacker has the ability to legitimately add or modify calendar files on a CalDAV server," the firm said in an advisory. The flaw was found on iCal 3.0.1 running on Mac OS X 10.5.1. Upgraded versions of the software are not affected.

Source:

http://www.betanews.com/article/iCal_bugs_can_lead_to_DoS_and_code_execution_attacks/1211469285

34. *May 21, Dark Reading* – (National) **'Hack-and-Pier' Phishing on the Rise.** Researchers have witnessed a growing trend in phishers hacking into legitimate Websites to host their phishing exploits, enabling them to keep their attacks alive longer. In a blog post Wednesday from F-Secure noted a series of so-called 'hack-and-pier' phishing exploits that had been reported to phishing clearinghouse PhishTank. "Instead of setting up their own sites, we're seeing more and more evidence of phishing from hacked sites; legitimate sites that are unknowingly hosting phishing," the blog said. "And then the site cannot simply be pulled offline without collateral damage to the legitimate business. So the Website's administrator must be contacted to repair the damage." According to MarkMonitor, only a small percentage of phishing sites today are created with purchased domain names or hosting. "A study we did in late 2007

showed that over 80 percent of phishing sites were hacked legitimate sites or free Webhosting sites,” says the director of anti-phishing for MarkMonitor. Traditionally, a phisher would register a bogus URL that looked a lot like the real thing, but was a letter or two off, such as “paypol” rather than “paypal,” or a more obscure URL that was less likely to get flagged. But those URLs can be easy to spot and shut down, so phishers have been moving to legit Websites as a way to extend the life of their exploits. An F-Secure representative said in an interview that his firm in the past has seen many examples of hacked legit sites for phishing and other cybercrime uses. “It is a growing trend,” he says. “Like any other technique, practice makes perfect.” As long as there are vulnerable Websites, hack-and-pier phishing isn’t going anywhere. “Until the Website’s vulnerabilities are resolved, the phishers will just continue to hack and pier,” he said.

Source: http://www.darkreading.com/document.asp?doc_id=154558

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

35. *May 22, IDG News Service* – (National) **Cisco patches router flaw ahead of rootkit talk.** Cisco has issued three security patches, fixing bugs that could crash its products and drawing a warning from the SANS Internet Storm Center. The updates, issued Wednesday, fix denial of service bugs in the SSH (Secure Shell) software in Cisco’s Internetwork Operating System (IOS), used to power its routers, and in the Cisco Service Control Engine, which provides carrier-grade networking services. Cisco has also patched a privilege escalation vulnerability in its Voice Portal automated telephone customer service software. In its security advisories Cisco said that all of the bugs had been discovered by its own researchers, but SANS warned that researchers are likely reverse-engineering the patches and may release exploit code publicly. These particular updates are getting extra attention from the security community, which is now closely investigating how malicious software might work on IOS, an operating system that has largely evaded serious scrutiny. On Thursday, for example, Core Security is slated to give a widely anticipated presentation on a Cisco rootkit it calls the DIK (Da Ios rootKit) at the EuSecWest conference in London. Cisco recently changed its software update policy, saying it will now only issue IOS patches in March and September each year, unless forced to rush out a fix for serious bugs that were publicly disclosed or which were being actively exploited.

Source: http://www.infoworld.com/article/08/05/22/Cisco-patches-router-flaw_1.html

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

Commercial Facilities Sector

Nothing to Report.

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

National Monuments & Icons Sector

36. *May 22, WKMG 6 Orlando* – (Florida) **‘Hell’ wildfire 20 percent contained.** In Florida, a fast-moving 1,000-acre wildfire that threatened to cut off hundreds of families from help as it burned around a community was 20 percent contained early Thursday. Mandatory evacuations of the Deerhaven community began Wednesday afternoon as flames jumped around a wooded area, sparking new fires. The cause of the fires is unknown.

Source: <http://www.local6.com/news/16353128/detail.html>

37. *May 21, CNN* – (National) **Civil rights school on list of 11 endangered sites.** An elementary school at the center of a civil rights battle, a hospital ravaged by Hurricane Katrina and a hangar that once housed U.S. Navy dirigibles are on this year’s National Trust for Historic Preservation’s endangered list. The 11 sites represent the country’s architectural, cultural and natural heritage, and “reflect extraordinary periods of American history,” the National Trust Director said. He said the list is designed to raise awareness. Endangerment does not necessarily mean the building is in the potential path of a bulldozer, according to the official. Lack of funding can be just as serious, as the case of the California state parks demonstrates. The sites are listed in alphabetical order: Boyd Theater, Philadelphia, Pennsylvania; California’s park system, Charity Hospital and adjacent neighborhood, New Orleans, Louisiana; Great Falls Portage, Great Falls, Montana; Hangar One, Moffett Field, Santa Clara County, California; Lower East Side, New York; Michigan Avenue Streetwall, Chicago, Illinois; Peace Bridge Neighborhood, Buffalo, New York; The Statler Hilton Hotel, Dallas, Texas; Sumner Elementary School, Topeka, Kansas; and Vizcaya and the Bonnet House, Florida

Source: <http://www.cnn.com/2008/US/05/21/endangered.historic.places/index.html>

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

Dams Sector

38. *May 21, Associated Press* – (Louisiana) **Leaky New Orleans levee alarms experts.** Despite more than \$22 million in repairs, a levee that broke with catastrophic effect during Hurricane Katrina is leaking again because of the mushy ground on which New Orleans was built, raising serious questions about the reliability of the city’s flood defenses. Outside engineering experts who have studied the project told The Associated Press that the type of seepage spotted at the 17th Street Canal in the Lakeview neighborhood afflicts other New Orleans levees, too, and could cause some of them to collapse during a storm. The Army Corps of Engineers has spent about \$4 billion so far of the \$14 billion set aside by Congress to repair and upgrade the metropolitan area’s hundreds of miles of levees by 2011. Some outside experts said the leak could mean that

billions more will be needed and that some of the work already completed may need to be redone. The Army Corps of Engineers disputed the experts' dire assessment. The agency said it is taking the risk of seepage into account and rebuilding the levees with an adequate margin of safety. Over the past few months, however, the corps found evidence that canal water is seeping through the joints in the sheet metal and then rising to the surface on the other side of the levee, forming puddles and other wet spots. Engineers said the boggy ground is a more serious problem than the corps realizes. An official said there is a roughly 40 percent chance of the 17th Street Canal levee collapsing if water rises higher than 6 feet above sea level. During Katrina, the water reached 7 feet in the canal. The chief of the corps' technical support branch in New Orleans denied the problem at the 17th Street Canal is serious.

Source: http://www.usatoday.com/news/nation/2008-05-21-levee-neworeleans-leak_N.htm

39. *May 21, Progress* – (Pennsylvania) **Montgomery Run Dam in need of repairs.** It will cost the Clearfield, Pennsylvania Municipal Authority (CMA) \$7.3 million to upgrade the Montgomery Run Dam, according to a CMA engineer. The Moose Creek Reservoir Dam, like many other dams in the area, needs to have its spillway upgraded to meet new state Department of Environmental Protection (DEP) regulations. To meet the new DEP regulations, the Montgomery Run Dam must be able to handle 35 inches of rainfall in a 72-hour period. Currently the dam can only handle 23 percent of this flow, according to the engineer. Additionally, a new, larger spillway will need to be constructed at the reservoir as well as an overflow spillway in case of high rain events. CMA will also have to armor the dam with roller compacted concrete to prevent erosion; these improvements are estimated to cost \$5.92 million, the official said. In addition to these improvements, he said there are three pipes, two 24-inch-diameter intake pipes and a 36-inch drainage pipe under the dam, which are a part of the original dam built in 1902. DEP has long been after CMA to upgrade the pipes and install additional control valves on them so they could be shut off at the dam in case they leak. If the pipes were to crack and leak, the escaping water could erode away the base of the dam and cause it to fail, he said. Currently CMA's shutoff valves for the pipes are downstream from the dam and not at the dam itself.

Source: <http://www.theprogressnews.com/default.asp?read=12532>

40. *May 21, Cumberland Times-News* – (Maryland) **Savage Dam is safe.** The inability to quickly fix a disabled release gate at Savage River Dam, Maryland, does not affect the safety of the structure, but could lead to full drainage of the reservoir during one of the next two winters so that repairs can take place, according to an official of the Upper Potomac River Commission. He said Tuesday that one of the dam's four release gates remains stuck in the down or closed position. The commission continues to await a consultant's report about the fitness of the gates at the dam. The official said it is possible that the report will show that more than one gate needs to be replaced.

Source: http://www.times-news.com/local/local_story_142093113.html

41. *May 21, Grand Junction Daily Sentinel* – (Colorado) **Dams ready to spill over.** In Colorado, the Blue Mesa Reservoir, the 29-mile long impoundment that tops the

Aspinall Unit of dams, is the key to controlling the torrent of snowmelt pouring out of the high country. The Bureau of Reclamation's Grand Junction office is charged with balancing water levels in the three Aspinall Unit dams — Blue Mesa, Morrow Point and Crystal, and its lead hydrologist said a May 15 runoff forecast predicted the April through July inflows to Blue Mesa at 40,000 acre-feet greater than previously estimated. "Right now we're looking at 1.1 million acre-feet, which is 153 percent of average," he said. That is more than Blue Mesa can hold, which means some of that water has to go downstream. Flows in the lower Gunnison Basin were expected to peak Wednesday or today, he said in an e-mail Wednesday. By the time the ramping is done, which might be Saturday or Sunday, there will be 6,000 to 7,000 cubic feet per second ripping through the Black Canyon and the Gunnison Gorge. By Wednesday afternoon, flows had increased to 4,250 cfs. To reach that level, the bureau will open the bypass tubes and produce maximum power generation at Blue Mesa and Morrow Point dams. That will send 6,500 cfs of water into Crystal Reservoir, and because that dam only can release 4,150 cfs through its bypass tubes and power plant, the rest will have to go over the top. "Crystal Reservoir is at a level at which it will begin spilling today," the official said, announcing an event that last occurred in 1997. Flows will increase by 800 cfs per day through Saturday. He said the spill is scheduled to go through May 31, but that could change depending on weather, water conditions at Delta and side inflows. The bureau is monitoring several main tributaries, including the Cimarron River, Crystal Creek and the Smith Fork, which is downstream of the dams but contributes to the water reaching Delta.

Source:

http://www.gjsentinel.com/news/content/news/stories/2008/05/21/052208_1a_gunnison_gorge.html

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

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov 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.