Department of Homeland Security Daily Open Source Infrastructure Report for 04 May 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Gwinnett Daily Post reports the state of Georgia is halting the sale of government surplus computers, after private citizens' personal information turned up on computers bought by a bargain hunter. (See item 8)

- The U.S. Government has released its pandemic flu plan that outlines exactly which government agency is responsible for some 300 tasks, and warns that the federal government won't be able to offer the kind of aid expected after one−time, one−location natural disasters. (See item 25)

- The Associated Press reports New Orleans Mayor Ray Nagin has unveiled a new evacuation strategy for the city that relies more on buses and trains, and eliminates the Superdome and Convention Center as shelters. (See item 28)

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 03, Victorville Daily Press (CA)* — **Company spills 500 gallons of fuel.** A jet fuel storage facility at Southern California Logistics Airport, located north of Los Angeles in Victorville, sprang a leak, dumping an estimated 500 gallons of fuel and cutting off fresh supplies to

Edwards Air Force Base, officials said. The facility is owned and operated by Kinder Morgan. Rick Rainey, a spokesperson for Kinder Morgan, was unable to say when the line to Edwards would be restored. The leak occurred at about 9:30 a.m. PDT Monday, May 1, in the 13300 block of Air Expressway Boulevard, Kim Clover, spokesperson for the Victorville Fire Department, said. She noted that the cause was a mechanical failure of a valve. Rainey said the leak is under investigation. He could not say if the leak was coming from one of the three tanks or one of the pipes associated with the terminal. "It is not a pipeline issue; it is a terminal issue," he said.
Source: http://www.vvdailypress.com/2006/114666130297234.html

2. *May 03, Suburban Chicago News* — **Explosion report backfires for tired refinery worker.** Instead of calling off of work, a tired, apparently overworked ExxonMobil worker called the police and claimed the plant at which he worked had blown up, police said. Lacey Richards, 33, was arrested on a felony charge of making a false fire alarm call. Richards, a forklift driver, was working a 12−hour shift and was "getting tired," and decided to call 911 on his cellular telephone and tell them there was an explosion at the plant. Dispatchers traced his cell phone number, called the plant, and discovered he was scheduled to be working at the plant that supposedly had blown up. Richards admitted he called in the phony explosion in hopes of going home early.
Source: http://www.suburbanchicagonews.com/heraldnews/city/4_1_JO03_EXPLOSION_S1.htm

3. *May 02, North American Electric Reliability Council* — **NERC adopts permanent cyber security standards.** The Board of Trustees of the North American Electric Reliability Council (NERC) on Tuesday, May 2, adopted eight new cyber security standards that address asset identification, security management controls, personnel and training, perimeter security, systems security, incident reporting and response planning, and recovery plans. These standards replace the Urgent Action Cyber Security Standard, which NERC adopted on an interim basis in August 2003 to address cyber security concerns in the wake of the September 11, 2001 terrorist attacks. “These eight new standards provide a comprehensive set of requirements to protect the bulk power system from malicious cyber attacks,” said Rick Sergel, NERC president and CEO. The security standards will become effective on June 1, 2006. In addition to the cyber security standards, the board approved 13 additional reliability standards that address interchange coordination; system restoration plans; data requirements, documentation, and reporting procedures; as well as an urgent action standard that addresses a Southwest Power Pool regional difference on inadvertent interchange. NERC will file all of the newly adopted standards with the U.S. Federal Energy Regulatory Commission and applicable governmental authorities in Canada. These standards are proposed to become electric reliability organization reliability standards once they are approved by U.S. and Canadian authorities.
Reliability standards:
ftp://www.nerc.com/pub/sys/all_updl/docs/bot/Agenda−Items−0506/Item5.pdf
Source: http://www.nerc.com/

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *May 02, Reuters* — **Senate backs funds for defense contractor hurricane losses.** The Senate on Tuesday, May 2, backed a plan to give Los Angeles−based Northrop Grumman Corp. up to $500 million for business disruptions at its Mississippi and Louisiana shipyards after last year's devastating hurricanes. The Northrop Grumman measure is intended to provide bridge funding while the company battles with its insurance company, Factory Mutual Insurance Co., in court about the money. It would require Northrop to reimburse the government when and if it won reimbursement from the insurance company. The White House and the U.S. Navy oppose the measure, which they say could set a dangerous precedent and decrease incentives for insurance companies to pay out claims. Senate Appropriations Committee, Senator Thad Cochran (R−MS) warned that without the emergency funds, the cost of future military contracts could escalate. The Navy fears that the measure could further raise the cost baseline for already expensive shipbuilding programs.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/05/02/AR2006050201376.html

5. *May 02, U.S. Department of Defense* — **Joint Forces Command focusing on current, future operations.** Air Force General Lance Smith told Pentagon reporters Tuesday, May 2, the top focus for the U.S. Joint Forces Command's (JFCOM) is supporting ongoing operations in Iraq and Afghanistan. A top priority for the command is improving the way military forces work together and with coalition partners, he said. While addressing these issues, JFCOM also is focused on ensuring interoperable command and control for units, agencies and organizations supporting a mission, Smith said. Another goal JFCOM is working on is "to marry intelligence and operations so they are closely linked," he said. Meanwhile, one of the most exciting initiatives at JFCOM is its focus on the future through its concept development and experimentation efforts, according to Smith. Industry and academia have proven to be solid partners in this effort and keys to the Department of Defense's transformation plans, he said.
Source: http://www.defenselink.mil/news/May2006/20060502_4995.html

[Return to top]

Banking and Finance Sector

6. *May 03, Denver Post* — **Man accused of giving ID data to neo−Nazis.** The former owner of a check−guarantee and debt−collection business was accused Tuesday, May 3, of turning over financial records of thousands of people to a neo−Nazi gang that authorities say engages in identity theft and other illegal activity. Robert Jerome Upson, 43, owner of the now−defunct Recovery Specialists Inc., which did business under the name of VeriCheck, appeared Tuesday in Denver District Court. Nine others also were indicted, including people identified as members and associates of the white supremacist Wood Pile Gang, which authorities say is related to the neo−Nazi Aryan Nations. The indictment said Upson turned over information about thousands of accounts to the identity−theft ring in exchange for drugs, money,

transportation, and lodging. As a result, VeriCheck clients and customers have lost more than $20,000, the indictment said. Police estimate that Upson's files contained up to 1.8 million personal and financial accounts. The goal of the group, which included Upson, was to obtain methamphetamine and steal money, merchandise, and services through identity theft, according to the indictment.
Source: http://www.denverpost.com/portlet/article/html/fragments/print_article.jsp?article=3777600

7. *May 03, Websense Security Labs* — **Phishing Alert: Yardville National Bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of Yardville National Bank, which serves New Jersey and Pennsylvania. Users receive a spoofed e−mail message, which claims that, due to multiple fraudulent activities, all customers are being asked to verify their accounts. This message provides a link to a phishing Website, which prompts users to enter account information to resolve the issue.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =479

8. *May 02, Gwinnett Daily Post (GA)* — **Personal info found on sold government computers.** The state of Georgia is halting the sale of government surplus computers, after private citizens' personal information turned up on computers bought by a bargain hunter. Joe Kim, director of legal service for the state Department of Administrative Services, said the sale of government surplus computers has been put on hold. Credit card numbers, birth dates, and Social Security numbers of citizens were still on the hard drives of computers which state workers failed to erase before they were sold, WSB−TV reported. More than 150 surplus computers were in one man's work shed.
Source: http://www.gwinnettdailypost.com/index.php?s=&url_channel_id=32&url_article_id=14588&url_subchannel_id=&change_well_id=2

9. *May 02, electricnews.net* — **Phishing scam targets Bank of Ireland.** Bank of Ireland customers have been hit by yet another phishing scam in the form of an e−mail asking users to update their security details. The fake security alert landed in inboxes on Friday, April 28, and may have fooled a number of customers into handing over their access codes and passwords, redirecting them to a website designed to collect the details. As of Tuesday, May 2, the fraudulent site appears to have been disabled. A spokesperson for the bank confirmed that it had received several calls from customers about the scam, and that some PINs had been changed. She described the perpetrators of the attacks as "smart," as it was launched on the Friday of a Bank Holiday weekend. The bank's spokesperson said that this was the third attack specifically targeted at its customers in the past 18 months. She said she was not aware of fraud being perpetrated on a Bank of Ireland customer as a result of these phishing scams.
Source: http://uk.news.yahoo.com/02052006/95/smart−phishing−scam−tar gets−boi.html

[Return to top]

Transportation and Border Security Sector

10. *May 03, New York Daily News* — **Thirty percent of New York's subway phones broken.** Nearly 30 percent of pay telephones in the New York subways don't work, according to a report

released on Tuesday, May 2. Previous Metropolitan Transit Authority (MTA) contracts with Verizon called for 95 percent of the phones to be fully functioning at all times. But the current contract only urges Verizon to make a "good faith effort" to fix the defects within 24 hours of being notified, according to a report by the Straphangers Campaign. "The MTA and Verizon should agree to keep a certain number of pay phones working," Straphangers Campaign coordinator Neysa Pranger said. Even with the rise in cell phone use, pay phones are still necessary −− particularly in emergencies, the campaign said. The Straphangers Campaign checked more than 1,200 subway pay phones. Nearly 30 percent had at least one defect, including no dial tone, a blocked coin slot or a broken handset.
Straphangers Campaign Website: http://www.straphangers.org/
Source: http://www.nydailynews.com/front/story/414407p−350237c.html

11. *May 03, Associated Press* — **FAA: Air traffic control transformation under way.** Radar and radio, used since World War II to track aircraft from the ground, will eventually give way to a new satellite−based navigation technology. Federal Aviation Administrator (FAA) Marion Blakey said developing a system based on the new technology is critical to the future of aviation. "It's the way we're going to be addressing the horrific congestion we expect to see," Blakey told reporters on Tuesday, May 2. Replacing the current radar−and−radio air traffic control system with one that relies on satellites will require billions of dollars and take up to 20 years, according to the FAA. The satellite−based system, known as automatic dependent surveillance broadcast, or ADSB, includes a cockpit locator that determines an aircraft's precise location using the Global Positioning System. Once per second, a transponder sends that information to a ground station, which relays it to air traffic control. Pilots can see the same visual display in the cockpit that air traffic controllers see on the ground, showing the aircraft's precise location as well as the weather and the location of other aircraft nearby. In addition, controllers will be able to track helicopters and private planes that now fly beneath the radar.
Source: http://www.cnn.com/2006/TRAVEL/05/03/faa.satellite.nav.ap/in dex.html

12. *May 03, New York Times* — **Armenian plane carrying 113 crashes into Black Sea.** An Armenian passenger plane crashed into the Black Sea Wednesday morning, May 3, as it approached the southern Russian resort city of Sochi. Airline and emergency officials reported that there were 113 passengers and crewmembers on board and that none appeared to have survived. The airliner, an Airbus 320 belonging to Armavia, was flying to Sochi from Armenia's capital, Yerevan, when it plunged into the sea, according to news agencies. The plane crashed more than three miles from the shore as it tried to land in stormy weather, the officials said. A spokesperson for Armavia told the official Russian Information Agency Novosti that dispatchers at Sochi's airport had initially refused the pilots permission to land because of heavy rain, forcing it to circle and try again.
Source: http://www.nytimes.com/2006/05/03/world/europe/03cnd−plane.h tml?hp&ex=1146715200&en=d3bcbce2838a4cd3&ei=5094&partner=hom epage

13. *May 03, Associated Press* — **U.S. authorities plug massive cross−border tunnel in San Diego.** A federal contractor dumped cement in a 35−foot hole Tuesday, May 2, to begin plugging the longest secret tunnel ever discovered along the U.S.−Mexico border. The massive tunnel discovered in January extended 2,400 feet from a warehouse near the Tijuana, Mexico airport to another warehouse in San Diego. It was lit, ventilated and went as deep as 90 feet. The contractor dug a hole where the tunnel crossed the border and plugged that one section

with cement at a cost of $15,000, said Lauren Mack, spokesperson for the Department of Homeland Security. Homeland Security plans to eventually fill the entire U.S. portion of the tunnel −− a passageway that runs the length of seven football fields under streets, sidewalks, and other warehouses.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/14483947.htm

14. *April 29, Boston Globe* — **MBTA seeks sharp fare hikes.** Subway, bus, and commuter rail fares would rise sharply under an overhaul proposed on Friday, April 28, by the Massachusetts Bay Transportation Authority (MBTA). Starting in January, subway and trolley fares would increase from $1.25 to $1.70, bus fares would go from 90 cents to $1.25, and most commuter rail passes would cost 22 percent more. The increases would take effect in January, after a series of public workshops and hearings that start May 15 and after the MBTA board votes in November or December. The proposed fare increases would bring the MBTA in line with several of the nation's other largest transit agencies. The fare hikes are projected to bring in $70 million more a year, enough for the MBTA to balance its budget as it contends with $8.1 billion in debt, deteriorating infrastructure, and declining state sales tax revenues that help fund the agency. The nation's fourth largest public transit system averages 1.1 million passenger boardings each workday on a network of subway and commuter rail trains, trolleys, buses, and ferries that extends across the Boston region.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/04/29/mbta_seeks_sharp_fare_hikes/

[Return to top]

Postal and Shipping Sector

15. *May 03, DMNews* — **U.S. Postal Service filed for an 8.5 percent rate increase.** The United States Postal Service on Wednesday, May 3, filed for an average 8.5 percent postal rate increase, Postmaster General John E. Potter told the USPS board of governors. The average increase means that some postal rates will be higher than 8.5 percent and some lower. The filing with the Postal Rate Commission also includes permission to issue a non−denominational First Class forever stamp to hedge against future rate increases. Among the increases planned, First Class mail will go up 7.1 percent to 42 cents, from the current 39 cents.
Press release: http://www.usps.com/communications/news/press/2006/pr06_032. pdf
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3670 4

[Return to top]

Agriculture Sector

16. *May 03, Southeast Farm Press* — **Legislation would establish Alabama animal ID program.** The Alabama State Legislature has passed a bill that would authorize the state's Department of Agriculture and Industries to develop and implement an animal identification database consistent with the U.S. Department of Agriculture's Animal Identification System. The state already has implemented a voluntary premises registration program, which is the initial step

toward a National Animal Identification System (NAIS). The legislation also provides for the confidentiality of information initially gathered by the Alabama Department of Agriculture and Industries as the department implements and maintains a database of animal identification in accord with the national system. NAIS is a cooperative state−federal−industry partnership to standardize and expand animal identification programs and practices to all livestock species and poultry. NAIS is being developed through the integration of three components −− premises identification, animal identification and animal tracking. The long−term goal of the NAIS is to provide animal health officials with the capability to identify all livestock and premises that have had direct contact with a disease of concern within 48 hours after discovery.
Alabama Department of Agriculture & Industries: http://www.agi.alabama.gov/
Source: http://southeastfarmpress.com/news/050306−Animal−ID/

17. *May 03, Ohio Ag Connection* — **Gypsy Moth quarantine area expands to 46 Ohio counties.** Ohio Department of Agriculture Director Fred L. Dailey Tuesday, May 2, announced an expansion of Ohio's quarantine area to include Franklin and Delaware Counties in an effort to prevent further spread of the gypsy moth, one of the most destructive hardwood forest pests in the United States. The quarantine prohibits movement of materials containing gypsy moth egg masses into or out of the county. Nursery producers who ship out of regulated areas must have each load of stock inspected and accompanied by a certificate verifying it is free of gypsy moths.
Ohio Department of Agriculture: http://www.ohioagriculture.gov/
Source: http://www.ohioagconnection.com/story−state.cfm?Id=254&yr=20 06

18. *May 02, U.S. Department of Agriculture* — **USDA releases May 2006 Cereal Rust Bulletin.** The U.S. Department of Agriculture's (USDA) Agricultural Research Service released its fourth Cereal Rust Bulletin for 2006 on Tuesday, May 2. Rusts are among the most damaging diseases of wheat and other small grain crops. Wheat is grown in nearly every state of the U.S., but the greatest concentration is in the Great Plains. The high concentration of wheat from central Texas to Minnesota and the Dakotas makes this region especially vulnerable to stem rust and leaf rust epidemics. The cereal rust fungi are superbly adapted for long distance spread. Rust epidemics start in fall−sown crops of winter wheat in the southern plains. Each rust infection in a wheat leaf or stem produces tens of thousands of spores that are released in the wind like pollen to produce new infections wherever they land on other susceptible wheat plants. Some spores establish new infections after traveling hundreds of miles in high altitude air currents. Within one to two weeks, each new infection begins releasing spores to initiate the next generation of infections.
Please refer to source to view the updated Cereal Rust Bulletin.
Cereal Rust Situation Reports and Bulletins:
http://www.ars.usda.gov/Main/docs.htm?docid=9757
Additional information was found at: http://www.ars.usda.gov/Main/docs.htm?docid=9854
Source: http://www.ars.usda.gov/SP2UserFiles/ad_hoc/36400500Cerealru stbulletins/06CRB4.pdf

[Return to top]

Food Sector

19. *May 03, USAgNet* — **New food safety Website launched.** Building on the successful Fight BAC! Campaign, the Partnership for Food Safety Education introduces a new Website dedicated to food−safety information. The new site features a wealth of food−safety information to help consumers reduce risk of food−borne illness.
Partnership for Food Safety Education's new Website: http://www.fightbac.org/
Source: http://www.usagnet.com/story−national.cfm?Id=805&yr=2006

20. *May 03, Food Production Daily (Europe)* — **European public skeptical of food safety measures, survey finds.** Recent food safety incidents and the introduction of genetically modified foods in Europe have resulted in public concern over the safety of the European food supply. According to a survey conducted by the European Union−funded Safe Foods Integrated Project, consumers have little confidence in the safety of their food supply and remain skeptical and distrustful of the management procedures currently in place. The implications of the study are that despite an increase in regulations and safeguards over the past five years, public concern remains high and could put further pressure on government to take additional measures. The food industry and regulators also need to do more to educate the media and the public about the issues, the report's authors suggest. The study also found the public may be suspicious of the motives behind particular measures.
Safe Foods Integrated Project Website: http://www.safefoods.nl/default.aspx
Safe Foods Integrated Project study:
http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6WB2−4JP9FN2−1&_coverDate=04%2F11%2F2006&_alid=390100438&_rdoc=1&_fmt=&_orig=search&_qd=1&_cdi=6698&_sort=d&view=c&_acct=C000026798&_version=1&_urlVersion=0&_userid=533256&md5=f248e0bfd2383c7876ec538577ff7a5c
Source: http://www.foodproductiondaily.com/news/ng.asp?n=67443−food−safety−media−confidence

21. *May 02, Cattle Network* — **USDA releases report on investigation into Alabama bovine spongiform encephalopathy case.** The U.S. Department of Agriculture's (USDA) Animal and Health and Inspection Service Tuesday, May 2, released the results of an investigation into a bovine spongiform encephalopathy (BSE) case identified in Alabama in March and noted that the animal was a non−ambulatory red crossbred, and that dentition determined that the animal was more than ten years old. The ten−year age determination is significant because it indicates that the animal was born prior to the implementation of Food and Drug Administration’s 1997 feed ban that minimizes the risk that a cow might consume feed contaminated with the agent thought to cause BSE.
Statement by USDA Chief Veterinary Officer John Clifford:
http://www.aphis.usda.gov/newsroom/content/2006/05/alepi.sht ml
Alabama BSE Investigation Final Epidemiology Report:
http://www.aphis.usda.gov/newsroom/hot_issues/bse/content/pr intable_version/EPI_Final.pdf
Source: http://www.cattlenetwork.com/content.asp?contentid=33818

[Return to top]

Water Sector

22. *May 02, Seattle Times* — **Seattle schools to turn water off; arsenic detected.** Drinking water is being shut off at all 100 Seattle public schools after tests last month found traces of arsenic in the water at several elementary schools. All of the fountains at the five schools with traces of arsenic had been shut for repairs before the arsenic was discovered. One −− at Van Asselt Elementary −− had been turned on again and had been operating for eight school days. The action comes just a few years after the district began a $13 million project to replace pipes and fixtures amid concerns over high levels of lead and iron in some faucets. The district will put bottled water in its schools. As the water is delivered over the next two weeks, the district will turn off drinking fountains. It's not clear where the arsenic came from. Seattle Public Utilities, which runs the city's water system, has tested its water for decades and never found more than a trace of arsenic, well below the allowable 10 parts per billion. The district planned to send letters to parents and make information available on its Website.
Seattle Public Schools Website: http://www.seattleschools.org
Source: http://seattletimes.nwsource.com/html/localnews/2002966029_w ater02m.html

23. *April 30, Indo−Asian News Service* — **Bicycle−powered water filtration system for disaster zones.** A bicycle powered portable water filtration system has been developed to save lives in a disaster zone, researchers said Friday, April 28. In Singapore, Nanyang Technological University's (NTU) institute of environmental science and engineering unveiled the unit, consisting of a bicycle coupled with a mechanical pump and a membrane module to filter the water. Believed to be the world's first, NTU experts said it is an improvement on the hand−cranked model made for Indonesia's tsunami−stricken Aceh Province in January last year.
Source: http://www.rxpgnews.com/medicalnews/healthcare/article_4190. shtml

[Return to top]

Public Health Sector

24. *May 03, Integrated Regional Information Networks* — **Egypt: Health ministry reports 13th human bird flu case.** A new human case of H5N1 avian influenza was announced on Tuesday, May 2, bringing the total number of reported human infections in Egypt to 13. A 27−year−old woman was diagnosed with the disease on Monday, May 1, after showing symptoms associated with the avian flu, according to the Ministry of Health. The infection is the first human case of the potentially fatal virus to have been reported within the capital, Cairo. According to the health ministry, the woman contracted the disease in her home village in the Menoufiya governorate, north of the capital, while handling sick domestic birds. Her condition is stable. Members of her family have tested negative for the illness. The discovery comes three days after a joint announcement by the health ministry and World Health Organization that there were no longer any human cases in Egypt. Egypt’s first human case was reported in mid−March. Since then, four people have died from the disease, while another eight have fully recovered.
Source: http://www.irinnews.org/report.asp?ReportID=53126&SelectRegi on=Middle_East&SelectCountry=EGYPT

25. *May 03, Reuters* — **Government releases pandemic flu plan.** A flu pandemic would cause massive disruptions lasting for months, and cities, states, and businesses must make plans now

to keep functioning −− and not count on a federal rescue. President Bush last fall proposed a $7.1 billion plan to prepare for the next worldwide outbreak of a super strain of influenza. This report updates that plan, an incremental step that basically outlines exactly which government agency is responsible for some 300 tasks, many already under way. Even draconian steps, such as shutting down U.S. borders against outbreaks abroad, would almost certainly fail to keep a flu pandemic from spreading here, the report acknowledges. In a severe pandemic, up to 40 percent of the work force could be off the job for two weeks. Because 85 percent of the systems that are vital to society are privately run, the administration aimed to use the report to energize businesses in particular to start planning how they will keep running under those conditions. The report warns that the federal government won't be able to offer the kind of aid expected after hurricanes or other one−time, one−location natural disasters.
Pandemic Influenza Implementation Plan:
http://www.whitehouse.gov/homeland/nspi_implementation.pdf
Fact Sheet: Advancing the Nation's Preparedness for Pandemic Influenza:
http://www.whitehouse.gov/ news/releases/2006/05/20060503−5.html
Source: http://www.nytimes.com/2006/05/03/health/03cnd−flu.html

[Return to top]

Government Sector

26. *May 02, News Channel 5 Network (TN)* — **Audit calls Tennessee state building security poor at best.** More than 10,000 state employees work in downtown Nashville, TN, and each one of them has an ID badge. A state audit released Tuesday, May 2, showed the security guards looking at those IDs haven't exactly been doing their jobs. The state conducted its check of security guards during May of last year. Auditors used fake IDs to see just how closely guards look at who should be coming into state buildings. Most of the time the auditors found the guards only glanced at the identification. The audit blamed the private security firm in charge, low wages, and a lack of training for the problem with the guards. Since this audit took place, the managers at the Department of General Services said they've made changes and tightened security at all state office buildings.
Source: http://www.newschannel5.com/content/news/18990.asp

[Return to top]

Emergency Services Sector

27. *May 02, New York Times* — **Hurricane protection plan flawed, engineers say.** The Army Corps of Engineers did not shift course to meet the needs of the changing landscape of New Orleans and so the city did not get the hurricane protection system that it needed, a panel of outside engineers said in a report released Tuesday, May 2. The corps did not follow its own procedures in monitoring the rate of subsiding and rising of water levels around the city, according to the report, and based the design of the levee system on outdated information that left floodwalls nearly two feet lower than they should have been. David E. Daniel, the chairman of the external review panel, said that the findings of the new report were consistent with what his panel had seen since the beginning of the process: "the hurricane protection system evolved

piecemeal over a period of time, with no one particular entity in charge of the whole system and no broad system−performance thinking exhibited in the design process," along with a tendency of "cutting too close to the margins" when it came to building in safety. The result, he said, was "gross catastrophic failure."
The report can be found at: http://www.asce.org/files/pdf/erp_progressreport.pdf
Source: http://www.nytimes.com/2006/05/02/us/03leveecnd.html?_r=1&hp &ex=1146628800&en=0fa82d4941321d88&ei=5094&partner=homepage& oref=slogin

28. *May 02, Associated Press* — **Mayor outlines New Orleans evacuation plan.** Mayor Ray Nagin unveiled a new evacuation strategy for New Orleans on Tuesday, May 2, that relies more on buses and trains and eliminates the Superdome and Convention Center as shelters. The Superdome and Morial Convention Center became a scene of misery for days after the August 29 hurricane as thousands of evacuees, many of them ill or elderly, languished with shortages of food and water. In the future, Nagin said, the Convention Center will be a staging point for evacuations, not a shelter. "Amtrak trains will also be used for evacuation purposes, which we're really excited about," Nagin said. He said Department of Homeland Security Secretary Michael Chertoff had cleared the way for the use of passenger trains. Nagin added that the city's communications infrastructure is being beefed up and that contingency for communication failures had been developed. The new plan also touches on a heart−wrenching decision evacuees faced ahead of Katrina: To board the buses, they had to leave their pets, and some refused to go without them. In the future, evacuees will be allowed to bring pets with them as long as they have some type of cage in which to safely put them.
Source: http://news.yahoo.com/s/ap/20060502/ap_on_re_us/new_orleans_ evacuations_5

29. *May 02, Associated Press* — **Texas 211 service to be part of hurricane readiness.** On Tuesday, May 2, Texas Governor Rick Perry announced the state's 211 service is being expanded to help those who can't evacuate during hurricanes and other disasters. The system will allow those affected people to register for transportation assistance.
Source: http://www.kxan.com/Global/story.asp?S=4848893&nav=0s3d

30. *May 02, Lahontan Valley News (NV)* — **Disaster planning drill will focus on flooding.** Although water officials in Nevada believe flooding can be averted this year as the heavy Sierra snowpack melts, an emergency action plan will be tested during an exercise in June. The Lahontan Dam Emergency Action Plan is an exercise that simulates dam failure, or water in excess of its capacity, at Lahontan Reservoir to prepare Churchill County officials for a potentially devastating event. Dave Overvold, project manager at the Truckee−Carson Irrigation District, said the table top exercise is sponsored by the Bureau of Reclamation and conducted once every five years. A simulated flood would prepare emergency agencies to evacuate residents and deal with the damage a major flood would cause. He said it is just a coincidence that this year's exercise is happening at a time when flooding is a concern because of the above average amount of snow−melt that will be pouring into Lahontan this spring and summer.
Source: http://www.lahontanvalleynews.com/article/20060502/News/1050 20025

31. *May 02, Government Technology* — **Federal, State and local government coordination for 2006 storm season.** The Department of Homeland Security announced recently the unprecedented predesignation of five teams that will coordinate the Federal government's role

in support of state and local governments in preparing for, and responding to, major natural disasters this storm season. In total, 27 Federal officials have been appointed, each with unique expertise and considerable experience. "Designating these teams now will give state and local officials a chance to plan, train, and exercise with their Federal counterparts before a disaster strikes," said Homeland Security Secretary Michael Chertoff.
Source: http://www.govtech.net/magazine/channel_story.php/99389

32. *May 02, Associated Press* — **Hybrid truck can serve as electricity generator during disaster recovery efforts.** The provider of the Army's heavy cargo−hauling Heavy Expanded Mobility Technical Truck vehicles is finishing up a prototype of an electric hybrid at the request of the Department of Defense. It not only increases gas mileage by about 20 percent from the standard three to four miles per gallon, it generates enough electricity to power a city block or hospital. Commercial vehicles such as garbage trucks and emergency vehicles all could benefit from using less fuel, says Gary Schmiedel, vice president of product engineering for Oshkosh Truck Corp. The technology has a storage system capturing energy that would otherwise be wasted in the braking process. The generator can produce up to 300 kilowatts of power −− enough to run 50 homes for an indefinite amount of time, he said. In response to Hurricane Katrina, Oshkosh took a hybrid truck to New Orleans and used it to pump out a hospital basement.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/05/02/AR2006050200848.html

[Return to top]

Information Technology and Telecommunications Sector

33. *May 02, Security Focus* — **Cisco Unity Express expired password privilege escalation vulnerability.** Cisco Unity Express (CUE) is prone to a privilege escalation vulnerability. Analysis: CUE contains a vulnerability that might allow an authenticated user to change the password for another user by using the HTTP management interface, if the password for the user being modified is marked as expired. This can result in a privilege escalation attack and complete administrative control of a CUE module, if the password being changed belongs to an administrator. An attacker could reset the password of a privileged account that has an expired password.
Vulnerable: Cisco Unity Express 2.2(2); Cisco Unity Express 2.1(1); Cisco Unity Express 1.1(1); Cisco Unity Express.
Solution: Fixes are available. Please see the referenced Cisco advisory for details:
http://www.cisco.com/warp/public/707/cisco−sa−20060501−cue.s html
Source: http://www.securityfocus.com/bid/17775/discuss

34. *May 02, Security Focus* — **MySQL remote information disclosure and buffer overflow vulnerabilities.** MySQL is susceptible to multiple remote vulnerabilities. Analysis: A buffer overflow vulnerability due to insufficient bounds checking of user supplied data before copying it to an insufficiently sized memory buffer. This issue allows remote attackers to execute arbitrary machine code in the context of affected database servers. Failed exploit attempts will likely crash the server, denying further service to legitimate users. Two information disclosure vulnerabilities due to insufficient input sanitization and bounds checking of user supplied data.

These issues allow remote users to gain access to potentially sensitive information that may aid them in further attacks.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/17780/info
Solution: The vendor has released version 5.0.21 of MySQL to address these issues. Versions 4.0.27, 4.1.19, and 5.1.10 are also scheduled to be released in the future.
For more information: http://www.securityfocus.com/bid/17780/references
Source: http://www.securityfocus.com/bid/17780/discuss

35. *May 02, Sophos* — **Vietnamese distributed denial−of−service hacking suspect arrested.** Sophos has announced news that a man has been arrested in Vietnam for launching a distributed denial−of−service attack against a commercial Website. The attack on Vietco's Website caused huge losses to the company. Nguyen Thanh Cong is suspected of beginning an attack on the Vietnamese e−commerce site, www.vietco.com, in March 2006. The Website, which has 67,000 regular members, auctions cell phones and other consumer electronics products. Cong faces charges for creating a Trojan horse that exploited a flaw in Microsoft's Internet Explorer. The Trojan horse, which is said to have been planted on a pornographic Website, turned unpatched computers into zombie PCs which were then ordered to repeatedly hit the Vietco site −− overwhelming its servers.
Source: http://www.sophos.com/pressoffice/news/articles/2006/05/viet ddos.html

36. *May 02, Sophos* — **Top ten malware threats and hoaxes reported to Sophos in April 2006.** Sophos has revealed the top ten malware threats and hoaxes causing problems for businesses around the world during the month of April 2006. The report, compiled from Sophos's global network of monitoring stations, reveals that Netsky−P, which recently celebrated its second birthday, has returned to the top of the virus chart, replacing Zafi−B. However, as a proportion of all malware, e−mail viruses and worms continue to decline −− 86 percent of the threats reported to Sophos during April were Trojan horses used by hackers to download malicious code, spy on users, steal information or gain unauthorized access to computers. The top ten viruses in April 2006 were as follows: W32/Netsky−P; W32/Zafi−B; W32/Nyxem−D; W32/MyDoom−AJ; W32/Netsky−D; W32/Mytob−FO; W32/Mytob−C; W32/Mytob−Z; W32/Dolebot−A; W32/Mytob−AS.
Source: http://www.sophos.com/pressoffice/news/articles/2006/05/topt enapr06.html

37. *May 02, IT Observer* — **WOW virus targets online gamers.** Security analysts at MicroWorld Technologies report that a new variant of the password stealing Trojan, named "Trojan−PSW.Win32.WOW.x," is spreading fast, attacking account holders of the online game "World of Warcraft." World of Warcraft is a multi−million dollar entity in the world of cyber games where huge sums change hands every second. Once the hacker gets hold of a gamer’s password, he can transfer victim’s goods to his personal account, which is easily converted to liquid currency through Gaming Currency Exchange Websites. MicroWorld experts have found that this Trojan slips into user computers via pop−up ads being displayed on many dubious gaming Websites, through a vulnerability in Internet Explorer.
Source: http://www.it−observer.com/news/6217/wow_virus_targets_onlin e_gamers/

38. *May 02, eWeek* — **Department of Homeland Security audit flags 'critical' Linux bug.** An open−source security audit program funded by the U.S. Department of Homeland Security has flagged a critical vulnerability in the X Window System which is used in Unix and Linux

systems. Coverity, the San Francisco−based company managing the project under a $1.25 million grant, described the flaw as the "biggest security vulnerability" found in the X Window System code since 2000. Coverity Chief Technical Officer Ben Chelf said the flaw resulted from a missing parenthesis on a small piece of the program that checked the ID of the user. It could be exploited to allow local users to execute code with root privileges, giving them the ability to overwrite system files or initiate denial−of−service attacks.
Source: http://www.eweek.com/article2/0,1895,1956652,00.asp

39. *May 02, Tech Web* — **Firefox updated with critical security fix.** Mozilla Corp. on Tuesday, May 2, released a patch for a zero−day critical security hole in Firefox that could be exploited to crash the browser or install malicious code. The flaw was found in Firefox 1.5.0.2.
Release notes for the Firefox 1.5.0.3 browser:
http://www.mozilla.com/firefox/releases/1.5.0.3.html
Source: http://www.informationweek.com/news/showArticle.jhtml;jsessionid=ME3EPJLH4VIDYQSNDBOCKHSCJUMEKJVN?articleID=187002829

40. *May 01, Dark Reading* — **SANS exposes 'safe' technologies.** For the first time, Mac OS X vulnerabilities ranked number one in the SANS Institute's quarterly Top 20 Internet Security Vulnerabilities report, which was published Monday, May 1. Experts at the SANS Institute said the vulnerabilities clarify an important point about non−Windows systems. "There's a difference between 'safer' and 'more secure,'" says Ed Skoudis, director of the SANS "Hacking Exploits" course curriculum and a senior security analyst at Intelguardians. "There are fewer users on systems like the Mac or Mozilla, which makes them less of a target for attackers, and therefore safer. But there's nothing inherent in those systems that makes them more secure."
SANS Top 20 Internet Security Vulnerabilities report:
http://www.sans.org/top20/2005/spring_2006_update.php
Source: http://www.darkreading.com/document.asp?doc_id=93759

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available, working exploit code for an unpatched vulnerability in Oracle Export Extensions. Successful exploitation may allow a remote attacker with some authentication credentials to execute arbitrary SQL statements with elevated privileges. This may allow an attacker to access and modify sensitive information within an Oracle database.

More information about this vulnerability can be found in the following:

Secunia Advisory19860

http://secunia.com/advisories/19860

Security Focus Oracle Vulnerability Report
http://www.securityfocus.com/bid/17699/discuss

Red Database Security Oracle Exploit Report
http://www.red−database−security.com/exploits/oracle−sql−injection−oracle−dbms_export_extension.html

US−CERT recommends the following actions to mitigate the security risks:

Restrict access to Oracle:
Only known and trusted users should be granted access to Oracle. Additionally, user accounts should be granted only those privileges needed to perform necessary tasks.

Change login credentials for default Oracle accounts:
Oracle creates numerous default accounts when it is installed. Upon installation, accounts that are not needed should be disabled and the login credentials for needed accounts should be changed.

Oracle has released Critical Patch Update April 2006. This update addresses more than thirty vulnerabilities in different Oracle products and components.
http://www.oracle.com/technology/deploy/security/pdf/cpuapr2 006.html

Phishing Scams
US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	38566 (−−−), 1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 50497 (−−−), 6348 (−−−), 135 (epmap), 55620 (−−−), 32459 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

41. *May 03, New York Times* — **Warehouse fire continues burning in Brooklyn.** A fire that roared through a network of abandoned, historic warehouses on the Brooklyn waterfront on Tuesday, May 2, continued burning Wednesday, May 3, with nearly 100 firefighters remaining on the scene to pump water on the smoking and smoldering remnants. The fire spread with a speed and ferocity that challenged and exhausted hundreds of firefighters, and led fire marshals to suspect arson. The blaze consumed a former rope factory on West Street near the site of the Continental Iron Works in Greenpoint, which launched the ironclad warship Monitor for the Union 144 years ago. More than 350 firefighters from at least 70 units spent all day Tuesday at the fire, those in front retreating to safety when entire walls crumbled and launched smoldering red bricks 100 feet down the narrow streets of the waterfront. At 10 alarms, it was called the city's largest fire in more than a decade, excepting the terrorist attacks of September 11, 2001. The fire area is a belt of formerly industrial, historic waterfront properties that are turning, one block at a time, into condominiums and apartments, bringing the young and affluent to the neighborhood, said Jennifer Givner, a spokesperson for the city's Department of Buildings.
Source: http://www.nytimes.com/2006/05/03/nyregion/03cnd−fire.html?hp&ex=1146715200&en=947819b831bba598&ei=5094&partner=homepage

42. *May 03, KGET TV17 (CA)* — **Concern grows over a leaking California dam.** The dam at Lake Isabella is one of the largest storage reservoirs in California and is now being watched closely by the U.S Army Corp of Engineers and local emergency personnel. The auxiliary dam at the west end of the reservoir is leaking and the rate of seepage has become a major concern. In fact, Kern County staffers discussed those concerns at a Board of Supervisors meeting on Tuesday, May 2. Water from the lake is seeping out of the dam at higher than normal rates. Then, there's an active fault line that runs beneath the dam, thought to be inactive when the dam was built in the early 1950's, dormant for hundreds of years, yet still a concern. And, considering the large population down river from the dam, namely Bakersfield, these trickling troubles have generated an undercurrent of concern. As an immediate precaution, the Corp of Engineers will lower the water level at sprawling reservoir by about two feet. The Army Corp of Engineers is also ramping up its inspections of the dam, and will be taking daily readings from moisture sensors in and around the dam and making visual inspections each day.
Source: http://www.kget.com/news/local/story.aspx?content_id=5027380C−398F−49E4−9A75−1173A247B9AE

43. *April 28, Federal Energy Regulatory Commission* — **FERC: Taum Sauk Project report.** The Taum Sauk Project is located in Reynolds County, MO, on the East Fork of the Black River approximately 90 miles southwest of St. Louis. The project is a reversible pumped storage project used to supplement the generation and transmission facilities of AmerenUE. This review examines the environmental impacts resulting from the breach of the upper reservoir rim dike at the Taum Sauk Pumped−Storage Hydroelectric Project operated by AmerenUE. On December 14, 2005, the northwest corner of the upper reservoir failed, releasing approximately 4,300 acre−feet of water in approximately one half hour. The water flowed down Proffit Mountain into the East Fork Black River, through a State Park and campground and into the lower reservoir. The following assessment is general in nature and the result of site visits, field interviews, public data filed with the Commission, Internet available information, and published accounts of the events. This report outlines the major environmental and

socio−economic effects of the flooding immediately following the event. The breach of the upper reservoir dike is described in detail in this report.
Taum Sauk Pumped Storage Project (No. P−2277) Dam Breach Incident Report:
http://www.ferc.gov/industries/hydropower/safety/projects/ta um−sauk/staff−rpt/full−rpt.pdf
Source: http://www.ferc.gov/industries/hydropower/safety/projects/ta um−sauk/staff−rpt.asp

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

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