Department of Homeland Security Daily Open Source Infrastructure Report for 25 May 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports federal officials said that sleep−deprived air traffic controllers may be partly responsible for two close calls on runways at Chicago's O'Hare International Airport. (See item 13)
- The Washington Post reports the World Health Organization may soon convene an expert panel to decide whether an unprecedented human outbreak of bird flu in Indonesia requires the world to go on higher alert for a possible pandemic. (See item 22)
- The Department of Homeland Security has launched the Ready Business Mentoring Initiative which includes business preparedness tools to help owners and managers of small− and medium−sized businesses prepare for emergencies. (See item 25)

DHS Daily Open Source Infrastructure Report *Fast Jump*

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 24, Reuters* — **Saudi, Conoco sign Yanbu refinery deal.** Saudi Aramco and U.S. oil firm ConocoPhillips signed a deal on Wednesday, May 24, for a 400,000 barrel−per−day (bpd), export−oriented refinery in the Gulf state, the second such agreement this week. The two refinery deals, valued at a total of $12 billion, are part of plans by Saudi Arabia, the world's

largest oil exporter, to become an increasingly important supplier of badly needed gasoline and heating fuel to global markets. The memorandum of understanding signed by Aramco and ConocoPhillips for the refinery in Yanbu on the Red Sea coast follows another signed on Sunday between Aramco and France's Total to build another 400,000 bpd, heavy crude refinery in Jubail on the kingdom's Gulf coast. State−run Aramco will supply the full−conversion refineries, targeted for start up in 2011, with 400,000 bpd of Arab heavy crude. The Yanbu refinery would produce high quality, ultra−low sulfur products that meet current and future U.S. and European specifications.
Source: http://www.nytimes.com/reuters/business/business−energy−cono co−saudi.html

2. *May 24, Charlotte Observer (NC)* — **Worker error led to power outage.** The loss of power Saturday, May 20, to the Catawba nuclear plant, leading to the shutdown of both its reactors, was a rare and unsettling event, experts say. Inaccurate settings by Duke Energy workers on electrical relays appear to have led to the break in power at the Lake Wylie plant less than 20 miles from uptown Charlotte, NC, a Nuclear Regulatory Commission (NRC) official said. The plant's two reactors automatically shut down, as they're supposed to, when electricity to the plant was interrupted. Duke declared an "unusual event," the lowest of four emergency stages. Diesel generators came on to circulate cooling water to the hot core and remove radioactive steam that remains bottled up in the plant after the reactors stop. The incident adds no risk to the public, an NRC official said. Catawba has a three percent to five percent chance of losing off−site power in a year, Duke's analyses predict.
Source: http://www.charlotte.com/mld/observer/news/local/14652518.ht m

3. *May 23, Toronto Sun (Canada)* — **Power cut to 8,000 homes; transformer fails in protest area.** A transformer station got caught in the crossfire of a native land dispute in Caledonia, Canada, on Monday, May 22, cutting power to nearly 8,000 homes. The transformer, located near the middle of the protest activity, malfunctioned and the lights went out in 1,546 homes in Caledonia and 6,377 homes in surrounding Norfolk. Repair crews were dispatched to the site immediately but couldn't penetrate the violent protest, blockades, and thousands of curiosity seekers who flocked to Caledonia during the day. Aboriginal protesters are using an electricity tower as part of their blockade and rumours circulated that a transformer station was set on fire. Plumes of smoke rose from the housing development at the heart of the dispute.
Source: http://torontosun.com/News/Canada/2006/05/23/1593123−sun.htm l

4. *May 23, Associated Press* — **Production remains down at St. Charles refinery.** The Valero St. Charles Refinery near Norco, LA, hasn't produced any low−sulfur diesel since an explosion and fire late Saturday, May 20, and its gasoline production is down 25 thousand barrels a day. The plant usually refines about 260 thousand barrels of oil a day. Company spokesperson Mary Rose Brown said Valero, the biggest U.S. refiner, expects gasoline production to return to normal and low sulphur diesel production to about ten thousand barrels a day when other units are restarted at the end of the week. The fire damaged a 48 thousand−barrel−a−day unit which removes sulfur, as well as some power and data transmission lines. Brown says the power and data line damage shut down five units: the crude and vacuum units, the coker, the naphtha hydrotreater and the reformer. Those were expected to be back in service within about a week.
Source: http://www.klfy.com/Global/story.asp?S=4939073

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *May 24, Government Accountability Office* — **GAO−06−537: Space Acquisitions: DoD Needs Additional Knowledge as it Embarks on a New Approach for Transformational Satellite Communications System (Report).** The Department of Defense (DoD) wants to create a networked force where soldiers and systems are able to operate together seamlessly. To help facilitate this transformation, DoD began the Transformational Satellite Communications System (TSAT) program in January 2004. The Government Accountability Office (GAO) reported in 2003 that TSAT was about to begin without sufficiently mature technology. In this report, GAO followed up with an assessment of (1) how the TSAT program is progressing, and (2) whether the program is using an acquisition approach that will provide the knowledge needed to enter product development. GAO is recommending that, before entering product development, DoD: (1) reassess the value of TSAT in broader context of other DoD investments, using updated knowledge on likely cost, schedule, technology, and initial capability; (2) update requirements in coordination with the TSAT user community; (3) demonstrate the maturity of all critical technologies; and (4) establish new cost, schedule, and performance goals. In commenting on the report, DoD agreed with the recommendations.
Highlights: http://www.gao.gov/highlights/d06537high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−537

[Return to top]

Banking and Finance Sector

6. *May 23, VNUNet* — **Panda launches phishing education campaign.** Security firm Panda Software launched a campaign this week designed to help surfers recognize and defend against phishing scams. Simple protection techniques listed in Panda's 10 Tips to Combat Phishing include typing URLs directly into the browser bar instead of accessing internet services through links. The April virus trends report from BlackSpider Technologies, another security vendor, found that the total number of virus−laden emails fell by 56 percent compared with March. Virus−infected emails now makes up just 0.79 percent of inbound emails. However, the Panda study found that the number of phishing emails in April rose by 35 percent compared with March, indicating that phishing attacks are becoming the more favored form of attack.
Source: http://www.vnunet.com/vnunet/news/2156679/panda−launches−phi shing

7. *May 23, WTRF−7 (WV)* — **Five arrested for check cashing scam.** The Fairmont, WV, police traveled to Roanoke, VA, to pick up five men, they say, who are involved in fraudulent check writing in the counties of Marion, Harrison, and Raleigh, WV. Fairmont police say the five men were part of a nationwide scheme to obtain stolen payroll checks and cash them illegally in Fairmont. In November of 2004, workers at WesBanco and First Exchange Bank in Fairmont

notified police of suspicious activity. Police say the men broke into a store to steal the checks and then went to area banks to cash them. The total damage was $40,000 in stolen money from Marion County alone.
Source: http://www.wtrf.com/story.cfm?func=viewstory&storyid=11107

8. *May 23, OUT−LAW News* — **Web conferencing tools can expose data.** SecureTest has warned that popular Web conferencing software can be used by hackers to gain direct access to the desktop of any PC on an internal network without detection, provided the hacker can buy the help of a jaded employee. SecureTest reported Monday, May 22, that Web conferencing sidesteps every security barrier an organization may have in place such as PKI, digital signatures, and SSL encryption, and is often not covered by the security policy. The hacker's accomplice need have no technical expertise. Anyone with access to a PC can route information out of the organization undetected. Unlike keylogging or physically downloading data onto a USB key, Web conferencing requires no special equipment or software planting, so it is the type of scam that would succeed where keylogging failed. To carry out a web conferencing attack, the insider logs on to a vendor portal before connecting to a third party conferencing portal. The hacker also connects to the portal, starting the Web conference. The insider allows the hacker to take remote control of his desktop and the hacker can now use the mouse to open files and directories. The discerning hacker can then identify data of interest and extract it.
Source: http://www.out−law.com/page−6945

9. *May 23, Finextra* — **New security device aims to protect chip and PIN users from shoulder surfers.** A new chip and PIN security device that has been designed to protect cardholders from "shoulder surfing" thieves at ATMs is being piloted by a UK health and beauty retailer. Researchers at Warwick University originally designed the device, which features a specially−designed magnifying lens, to help visually impaired customers see the keys on a chip and PIN terminal. But the device is now being marketed to retailers and banks after it was realized that only the customer directly in front of the lens could view the keypad clearly. The lens distorts the view of the keypad from any other angle and so allows PINs to be protected from shoulder surfing criminals or hidden cameras.
Source: http://finextra.com/fullstory.asp?id=15349

10. *May 21, Websense Security Labs* — **Multiple Phishing Alert: ViewPoint Bank and Phoenix Federal Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of ViewPoint bank, which is based in Texas. Users receive a spoofed e−mail message, which claims that their Internet banking services are due for renewal and will be cancelled if action is not taken immediately. This message provides a link to a phishing Website, which prompts users to enter account information to resolve the issue. Another new phishing attack targets customers of Phoenix Federal Credit Union, which has locations in Connecticut and New York. Users receive a spoofed e−mail message, which claims that their Internet banking services are due for renewal and will be cancelled if action is not taken immediately. This message provides a link to a phishing Website, which prompts users to enter account information to resolve the issue.
ViewPoint Bank screenshot: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=495
Phoenix Federal Credit Union screenshot:
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =496

Source: http://www.websensesecuritylabs.com/alerts/

[Return to top]

Transportation and Border Security Sector

11. *May 24, Transportation Security Administration* — **TSA prepares for busiest summer travel season on record.** The Transportation Security Administration (TSA) on Wednesday, May 24, announced it has prepared its workforce and airport operations to ensure the highest levels of security and customer service for travelers this busy summer travel season. TSA also reminds travelers to plan ahead, using the resources available on the TSA Website, including travel tips, airport−by−airport wait times during peak hours, and a detailed list of prohibited items. Officials from TSA, airports and major airlines anticipate 200 million air travelers nationwide during the peak summer travel period between the Memorial Day and Labor Day weekends. "This will be one of the busiest travel seasons on record and TSA will be ready," said Kip Hawley, said Assistant Secretary of Homeland Security for TSA.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 01e44a1

12. *May 24, Associated Press* — **Denver airport to rearrange gates, build jet facility for United, Frontier.** Denver International Airport (DIA) will reconfigure some of its gates and construct a $41.5 million regional jet facility to allow its two largest carriers to increase services to the city, the airport announced Tuesday, May 23. Under the deal, United Airlines will stop using six gates on Concourse A during the next year and move into five gates on Concourse B, where the airport's largest carrier operates most of its flights. In exchange, DIA will build the jet facility for United on the east end of Concourse B. United and the airport had agreed to build a much larger facility in 2003, but stopped the project amid industry turmoil. DIA also will retire $110 million in debt for the now−demolished automated baggage system equipment, which United stopped using last year −− decreasing the airline's airport costs. Frontier Airlines will lease the newly open gates on Concourse A, which the airport said would allow for more growth without having to expand the concourse. United and Frontier account for more than 77 percent of DIA's passengers.
Source: http://www.usatoday.com/travel/flights/2006−05−24−denver−upg rades_x.htm

13. *May 24, Associated Press* — **Officials: Tired air traffic controllers may be cause of Chicago runway mishaps.** Sleep−deprived air traffic controllers may be partly responsible for two close calls on runways at O'Hare International Airport, federal officials said. The incidents were part of a recurring pattern of fatigue for controllers at O'Hare, where officials were urged to "emphasize the importance of sleep management" in a letter from National Transportation Safety Board (NTSB) to the Federal Aviation Administration (FAA). On March 21, a Lufthansa plane and a Delta jet were mistakenly instructed to take off at the same time on crisscrossing runways. The planes came within 100 feet before the pilots were alerted and stopped. The controller was in training and had an untreated sleep disorder, authorities said. Two days later, planes from United Airlines and its low−cost carrier, Ted, came within 600 feet of each other when one plane was sent to taxi across a runway where the other had started its takeoff roll. That controller had just four hours of sleep, and told NTSB investigators that he "was not as sharp as (he) could have been," the letter said. The FAA found that both incidents were caused by controller errors.

Source: http://www.usatoday.com/travel/flights/2006−05−24−air−traffi c−mishaps_x.htm

14. *May 24, CNN* — **Blaze engulfs Istanbul airport.** A massive fire that engulfed part of Istanbul's Ataturk International airport left three people injured but did not cause major air traffic delays, Turkish officials said on Wednesday, May 24. Turkey's Deputy Governor Fikret Kasapoglu said that three people suffered smoke inhalation but there were no other casualties. He said the fire was believed to have been caused by a short circuit of electrical systems in a cargo area of the airport, and may have caused secondary explosions causing the fire to quickly spread. NTV television reported that the fire began in a section where fuel depots were located. Electrical work was being carried out at the time, one witness said. Thousands of people were forced to flee from the blaze as thick plumes of smoke and giant orange flames rose 100 feet into the air. Aided by winds blowing in the opposite direction, hundreds of firefighters worked to keep the flames away from a building near the cargo area that contained fuel tanks. An airport worker said computer systems were shut down, but flights were continuing, with workers using manual systems to check people in and out. Priority was being given to landing planes and delays were expected for departures, she said.
Source: http://www.cnn.com/2006/WORLD/europe/05/24/turkey.fire/index .html

15. *May 23, Daily Breeze (CA)* — **Los Angeles International Airport may offer security shortcut for frequent fliers.** Los Angeles International Airport (LAX) would offer some travelers a fast pass through security under a long−awaited program it hopes to launch by the end of the year. The program, known as Registered Traveler, would create express lanes through airport security for card−carrying travelers who have passed special background checks. The federal Transportation Security Administration (TSA) plans to establish the program on a trial basis in as many as 20 airports in the coming months. LAX would be an important proving ground for Registered Traveler because it screens more passengers on any given day than any airport in the country. An ongoing pilot program at Orlando International Airport has enrolled more than 20,000 registered travelers at $80 a year each. Los Angeles officials believe LAX could register 10 times that many travelers.
Source: http://www.dailybreeze.com/news/articles/2852951.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

16. *May 24, Agricultural Research Service* — **Novel antimicrobials protect against mastitis−causing bacteria.** An Agricultural Research Service (ARS) led team has combined specific DNA segments from two different sources to produce a novel antimicrobial protein. The resulting "fusion" antimicrobial protein degrades the cell walls of several bacterial pathogens in a solution of whey extracted from cow's milk. Agriculturally, the technology provides a key step to developing dairy cows that have a natural, built−in defense against

mastitis −− a disease that costs U.S. dairy producers up to two billion dollars annually.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

17. *May 24, Associated Press* — **Fruit fly find prompts quarantine.** Fresno, CA, officials have asked the state to impose a produce quarantine in a swath of America's most productive farmland after the discovery of six tiny fruit flies that can destroy fruits and vegetables. This would be the first quarantine in Fresno County in two decades. It is blamed on the discovery of the peach fruit fly, which can ruin about 50 types of tree fruit as well as some vegetables. Farms in an 85−square mile zone will be sprayed with pesticides and shipments will face inspections. The county is waiting for state approval before setting the boundaries of the quarantine, Fresno County Agriculture Commissioner Jerry Prieto said. The quarantine must last through two life cycles of the fly, or about two months.
Source: http://www.montereyherald.com/mld/montereyherald/news/146543 46.htm

18. *May 22, Lufkin Daily News (TX)* — **About 60,000 chickens dead after power outage.** About 60,000 five−pound birds died following a power outage Friday, May 19, at Texas' Stephen F. Austin (SFA) State University broiler farm, at a cost of about $90,000 to Pilgrim's Pride and about $30,000 to the SFA Broiler Research Center. Joey Bray, broiler farm manager, and Tim Cherry, director of the poultry science program, attributed the "massive die−off" to a failure of all standard back−up systems that should have started the generator or called the phone numbers on the "Sensaphone" −− a remote thermostat monitoring system.
Source: http://www.lufkindailynews.com/news/content/news/stories/2006/05/23/Dead_chickens.html?cxtype=rss&cxsvc=7&cxcat=9

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

19. *May 24, Ruidoso News (NM)* — **Village declares water emergency.** Reacting to news that Grindstone Reservoir dropped to only a 234−day water supply, that the flow of the river that feeds it is low and that village wells aren't producing sufficiently, Ruidoso, NM, councilors Friday, May 19, declared a state of water emergency. Using that declaration as a base, they imposed Phase five water restrictions, the strictest on the books, and a temporary moratorium on new developments and site plans. Village Water Director Ken Mosley called conditions "the worst" he has seen, with little run−off to the Rio Ruidoso because of lack of snow last winter and sparse rainfall this spring.
Source: http://www.ruidosonews.com/apps/pbcs.dll/article?AID=/20060524/NEWS01/605240301/1001

20. *May 24, Portland Press Herald (ME)* — **A week after flooding, safety of well water is still a concern.** Some Maine residents who rely on private well water have resorted to boiling their

water and buying bottled water while they wait to learn if their own supply is safe. State officials suspect that some York County wells were contaminated during last week's flooding, and they're encouraging people whose water has an unusual taste or odor to get it tested. Flood victims whose entire wells were under water are also being asked to do testing. Hundreds of test kits have been distributed since last weekend, and more will be available Wednesday, May 24. Test results won't be available for at least two days. In the meantime, concerned residents are being asked to take precautions.
Source: http://pressherald.mainetoday.com/news/york/060524water.shtm l

[Return to top]

Public Health Sector

21. *May 24, Agence France−Presse* — **China reports two new avian flu outbreaks among migratory birds.** China reported two new outbreaks of avian flu among migratory birds, bringing to four the number of such cases recorded in the northwest over the past month. A total of 399 bar−headed geese and ruddy shelducks had died from the virus in outbreaks in Tibet's Naqu district and the Guoluo Tibetan Autonomous Prefecture in neighboring Qinghai province, the agriculture ministry said. The ministry reported that the outbreaks were confirmed as the H5N1 virus Wednesday, May 24. Although the two outbreaks had occurred in separate locations, they were linked by the same migratory route. The route also linked the outbreaks to two other recent incidents in the area, the ministry said.
Source: http://www.forbes.com/home/feeds/afx/2006/05/24/afx2769641.h tml

22. *May 24, Washington Post* — **Bird flu alert level for Indonesia may increase.** The World Health Organization (WHO) may soon convene an expert panel to decide whether an unprecedented human outbreak of bird flu in Indonesia requires the world to go on higher alert for a possible pandemic, health officials said Wednesday, May 24. If the global alert status were increased, it could entail the deployment of international stockpiles of anti−viral drugs to Indonesia and heightened monitoring of travel from the country to contain the outbreak. WHO's internal discussions over the alert level come after Indonesian health authorities confirmed that the H5N1 virus had killed at least six members from a single extended family on Sumatra island. A seventh family member also died from what investigators suspect was bird flu but she was buried before samples could be taken. Another relative is hospitalized with a confirmed case but is recovering. Maria Cheng, a WHO spokesperson, said the outbreak in the North Sumatran village of Kubu Sembilang, was not only the largest bird flu cluster in the world but also the first in which investigators believe the virus was passed from one person to another and then to third.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/05/24/AR2006052401271.html

23. *May 23, Government Health IT* — **Health and Human Services seeks ideas for saving personal data.** The U.S. Department of Health and Human Services (HHS) is looking for solutions through which people could store personal information electronically for use during emergencies. Such information would make it easier for individuals or their family members to get such things as federal assistance, medical treatment and insurance benefits. The HHS request for information is a result of lessons learned from last year’s storms. Some 1.5 million

people were affected and the loss of important documents by individuals, businesses and government considerably slowed the time it took to get relief to them.
Source: http://govhealthit.com/article94618−05−23−06−Web

24. *May 23, Agence France−Presse* — **British scientists working on faster virus detection.** British scientists are developing a single test that could spot more than 600 deadly viruses, including bird flu, rabies and foot and mouth disease, within hours, the government announced. It is hoped the so−called "Lab on a Chip" −− laboratory on a microchip −− will be able to detect diseases in up to 36 hours, much faster than current methods of confirming viruses, which can take as long as seven to 10 days. The Department for the Environment, Food and Rural Affairs (DEFRA) is pumping $2.8 million into the project as a key line of defense against possible future health scares. The test works by placing DNA extracts from the unidentified virus onto a chip covered with samples of DNA from known conditions. Depending on where the DNA "sticks", scientists can then determine the unidentified virus. The whole process takes from just a few hours to 36 hours.
Source: http://news.yahoo.com/s/afp/20060523/hl_afp/britainhealthresearch_060523191420;_ylt=ArqeUgqL9_uLVDRO9g6UKsqJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

[Return to top]

Government Sector

25. *May 24, Department of Homeland Security* — **DHS launches Ready Business Mentoring Initiative for hurricane season.** Designed as a call−to−action for business leaders, the Department of Homeland Security (DHS) on Wednesday, May 24, launched the Ready Business Mentoring Initiative. This effort includes the Ready Business Mentoring Guides and other business preparedness tools to help owners and managers of small− and medium−sized businesses prepare for emergencies. Homeland Security, in collaboration with the Department of Commerce, Small Business Administration, U.S. Department of Agriculture, and the nation’s leading business organizations, will distribute the Ready Business Mentoring Guides and other materials as the 2006 hurricane season approaches. Ready Business Mentoring Guides are comprised of two workbooks, the Mentor Edition and the User Edition. Each guide consists of more than 50 pages of step−by−step information designed to teach business owners and managers about affordable ways to better protect their businesses. The materials enable businesses to create and execute an emergency preparedness plan.
Individuals interested in more information about family and business preparedness can visit http://www.ready.gov or call 1−800−BE−READY to receive a "Get Ready Now” brochure.
Source: http://www.dhs.gov/dhspublic/display?content=5648

[Return to top]

Emergency Services Sector

26. *May 24, New York Times* — **New Orleans preps for the upcoming hurricane season.** Though it was fictitious, "Hurricane Alicia" offered state and federal officials gathered in New Orleans,

LA, Tuesday, May 23, an opportunity to test new plans for evacuating and sheltering thousands of people fleeing a major Gulf storm. Officials hope the blueprint, which was put into practice in a statewide drill, will eliminate at least some of the bedlam that the region endured during Hurricanes Katrina and Rita last year. Tony Robinson, regional director of response and recovery for the Federal Emergency Management Agency, said that several signs suggested the new initiatives would be an improvement. Armbands and bar codes were used to track "evacuees." Plans to use rail lines, commercial air travel and military buses to move people out of harm's way are in the works. In addition, officials added that a permanent shelter in northern Louisiana was being designed specifically for evacuees, with special−needs shelters already in place to provide medical care and help evacuees in housing pets.
Source: http://www.nytimes.com/2006/05/24/us/24evacuate.html?_r=1&or ef=slogin

27. *May 24, South Florida Sun−Sentinel* — **Report reveals more seniors need help fleeing storms.** A quarter of seniors age 75 and older would not be able to evacuate before a hurricane on their own −− statistics that suggest almost 340,000 elder Floridians might not be able to get food, medicine and the care they need in the event of a storm, according to an American Association of Retired Persons (AARP) report released Tuesday, May 23. The report, "We Can Do Better," drew on what happened during Hurricane Katrina. In Louisiana, 71 percent of the victims were older than 60, according to the report −− at least 68 died in nursing homes, some abandoned by their caretakers. Harris Interactive surveyed 1,648 older adults nationwide for the report, asking about their ability to evacuate. Researchers say the results suggest 13 million Americans age 50 and older would require help to flee from a natural disaster. Half of them will need it from someone outside their households.
The full report: http://assets.aarp.org/rgcenter/il/better.pdf
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−hlpe vacuate24may24,0,1457171.story?coll=sfla−home−headlines

28. *May 24, Associated Press* — **Mock evacuation drill in Louisiana canceled.** A mock evacuation that was supposed to be part of a two−day statewide hurricane preparedness drill in Louisiana was canceled after a misunderstanding about who had jurisdiction over a Federal Emergency Management Agency (FEMA) trailer park. The two−day statewide drill that began Tuesday, May 23, was aimed at avoiding the chaos that followed last year's deadly Hurricane Katrina. The mock evacuation was to take place in the state's largest FEMA trailer park in Baker, 10 miles from Baton Rouge. But the Baker evacuation was canceled because of an apparent communication breakdown, said JoAnne Moreau, director of the East Baton Rouge Parish Office of Homeland Security and Emergency Preparedness. "We were unable to get any information from the state or federal government on what policies or procedures were for evacuating those sites −− whose jurisdiction it was," Moreau said.
Source: http://hosted.ap.org/dynamic/stories/E/EVACUATING_NEW_ORLEAN S?SITE=7219&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2006−05−24−0 6−22−53

29. *May 23, GovExec* — **FEMA says it will meet hiring goals by hurricane season.** At a briefing Tuesday, May 23, Federal Emergency Management Agency (FEMA) and Department of Homeland Security officials said that with better planning, they expect a more coordinated response than ever to storms during the upcoming hurricane season. FEMA Acting Director R. David Paulison, whose confirmation hearing took place Wednesday, May 24, said the agency

has improved from the 73 percent staffing capacity reported in a study issued last week. He said FEMA has 85 percent of the employees it needs and is en route to hiring to 95 percent by the beginning of this year's hurricane season beginning Thursday, June 1.
Source: http://www.govexec.com/story_page.cfm?articleid=34152&dcn=to daysnews

30. *May 23, Federal Computer Week* — **Federal agencies have fixed many technology gaps for the upcoming hurricane season.** With less than a week to go before the 2006 hurricane season starts, federal civilian and military agencies have fixed many of the technology holes they faced last year, senior officials at the Departments of Homeland Security (DHS) and Defense (DoD) said Tuesday, May 23. The Federal Emergency Management Agency has fixed most of the information technology deficiencies outlined in Government Accountability Office reports, said David Paulison, FEMA's acting director. Interoperable communications among federal, state, local and military responders are now robust, said Army Lt. Gen. Steven Blum, chief of the National Guard Bureau. In addition, DHS has mapped out the federal, state and local communications architecture to know what can be affected and how to work around what is knocked out, said George Foresman, DHS Under Secretary for Preparedness.
Source: http://www.fcw.com/article94622−05−23−06−Web

[Return to top]

Information Technology and Telecommunications Sector

31. *May 23, Security Tracker* — **HP Software Distributor lets local users gain elevated privileges.** A vulnerability was reported in HP Software Distributor on HP−UX. Analysis: A local user can gain elevated privileges. The application contains unspecified vulnerabilities. No details were provided.
Solution: The vendor has issued fixes available at: http://itrc.hp.com
The HP advisory is available at:
http://www2.itrc.hp.com/service/cki/docDisplay.do?docId=c006 59649
Source: http://securitytracker.com/alerts/2006/May/1016139.html

32. *May 23, Security Focus* — **Sun Java Runtime Environment nested array objects denial−of−service vulnerability.** The Sun Java Runtime Environment is vulnerable to a denial−of−service vulnerability. This issue is due to the software's failure to handle exceptional conditions. Analysis: This issue is reported to affect Java Runtime Environment versions up to 1.4.2_11 and 1.5.0_06. This issue will crash Internet browsers running an affected Java plug in. An attacker may exploit this issue to cause a vulnerable application as well as all processes spawned from the application to crash, denying service to legitimate users. Due to the scope of the crash, data loss may occur.
A complete list of vulnerable products is available at:
http://www.securityfocus.com/bid/18058/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18058/references

33. *May 23, Security Focus* — **Sun ONE Directory Server remote denial−of−service vulnerability.** Sun ONE Directory Server is prone to a remote denial−of−service vulnerability.

Analysis: This issue is due to the application's failure to handle malformed network traffic. This issue allows remote attackers to crash the application, denying service to legitimate users.
Vulnerable products: Sun ONE Directory Server 5.2 Patch 4; Sun ONE Directory Server 5.2 Patch 3; Sun ONE Directory Server 5.2; Sun Java System Directory Server 5.2 Patch 2; Sun Java System Directory Server 5.2 2005Q4; Sun Java System Directory Server 5.2 2005Q1; Sun Java System Directory Server 5.2 2004Q2; Sun Java System Directory Server 5.2 2003Q4; Sun Java System Directory Server 5.2.
Solution: Sun has released patch 122476−01 to address this issue in Sun Java System Directory Server 5 2005Q4 (Native Package) and Sun Java System Directory Server 5.2 Patch 4 (Compressed Archive).
Sun 122476−01 patch: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds:docid:1−21−122476−01−1
Source: http://www.securityfocus.com/bid/16550/discuss

34. *May 23, eWeek* — **Microsoft: Use MS Word in safe mode.** Microsoft is advising users to begin using MS Word in safe mode to protect against targeted zero−day attacks. In the absence of a patch, independent security researcher Matthew Murphy has released a registry script fix that sets a Software Restriction Policy that runs any instance of 'winword.exe' with the 'Basic User' policy. Because the current attack vector requires that the target is running the admin rights, the implementation of software restriction policies can reduce the effects the attack. Microsoft's advisory also contains step−by−step instructions for running the vulnerable Word 2002 and Word 2003 in safe mode. The company is recommending that users first disable the Outlook feature to use Word as the default mail editor before changing settings to run Word in safe mode.
Microsoft pre−patch advisory: http://www.microsoft.com/technet/security/advisory/919637.mspx
Source: http://www.eweek.com/article2/0,1895,1966730,00.asp

35. *May 22, CRN* — **Microsoft Word attacks likely to continue.** Researchers at the SANS Institute’s Internet Storm Center on Monday, May 22, issued recommendations for organizations looking to protect their networks from zero−day attacks that use Microsoft Word files. The Word vulnerability is considered "highly critical" because it's difficult for organizations to block all Word documents in e−mail. To address the threats until Microsoft issues a patch, the SANS Internet Storm Center recommends that organizations use an e−mail system that quarantines attachments for at least six to 12 hours to allow antivirus signatures to catch up. It also suggests setting limits on user administration rights, using proxy servers to control sites accessible to internal users, and employing intrusion−detection systems and firewalls to monitor outbound traffic.
Source: http://www.crn.com/sections/microsoft/microsoft.jhtml;jsessionid=5FQVOT2IMCFBEQSNDBCSKH0CJUMEKJVN?articleId=188101124

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 currently researching a zero−day vulnerability in Microsoft Word. In order for this exploit to be carried out, a user must first open a malicious Word document attached to an email or otherwise provided to them by an attacker. When the document is opened, malicious code is installed on the user's machine. The exploit then attempts to connect to a remote host. US−CERT and Microsoft will continue to investigate the public reports to help provide additional guidance as necessary. There is currently no patch available for this vulnerability.

For more information please review the following:

TA06−139A Microsoft Word Vulnerability:
http://www.us−cert.gov/cas/techalerts/TA06−139A.html

VU#446012 Microsoft Word buffer overflow: http://www.kb.cert.org/vuls/id/446012

Cyber Security Tip: http://www.us−cert.gov/cas/tips/ST04−010.html

Microsoft Security Advisory (919637):
http://www.microsoft.com/technet/security/advisory/919637.ms px#EAF

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

Install anti−virus software, and keep its virus signature files up to date

Block executable and unknown file types at the email gateway

US−CERT strongly encourages Federal Agencies to educate their user base and constituency about the risk of opening unknown attachments from unknown sources even if sent by a known and trusted source.

We will continue to update current activity as more information becomes available.

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	1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 16802 (−−−), 38566 (−−−), 50497 (−−−), 27482 (−−−), 445 (microsoft−ds), 32779 (sometimes−rpc21), 49200 (−−−) 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

36. *May 24, Associated Press* — **Destroyed in 9/11 attacks, first rebuilt skyscraper opens.** The first destroyed skyscraper to be rebuilt since the September 11 attacks opened for business with state−of−the−art security features and few tenants, but was celebrated as a symbol of downtown resurgence. Developer Larry Silverstein officially opened the 52−story skyscraper for business Tuesday, May 23. The building was the third to collapse on September 11, 2001, after the twin towers. Like the trade center, it is owned by the Port Authority of New York and New Jersey and leased by Silverstein. The building is narrower and lets in more sunlight than its original version. Following recommendations to make high−rises safer and sturdier after the terrorist attacks, the skyscraper adheres to "a set of standards unique to any high−rise office building in America," said Silverstein. It also has adopted newer safety standards, with wider stairwells and two−foot−thick concrete walls.
Source: http://www.usatoday.com/news/nation/2006−05−24−tower_x.htm

37. *May 24, Associated Press* — **Suspected mercury contamination shuts down school, UNC library.** A Durham, NC, elementary school was closed on Wednesday, May 24, as officials investigated a possible mercury spill. Investigators also shut down a library at the University of North Carolina (UNC) at Chapel Hill for two hours Wednesday to investigate possible mercury contamination linked to a janitor who works at both campuses. Health officials believe Jesse McCrimon may have been exposed to mercury Tuesday while cleaning Oak Grove Elementary School in Durham. They initially believed he might have taken it to Davis Library at UNC Chapel Hill while working the overnight shift, said Derek Poarch, the university's police chief. Durham police said some students had found a "very small" spill at Oak Grove and that a student might have brought the mercury to the campus in a water gun.
Source: http://www.hendersonvillenews.com/apps/pbcs.dll/article?AID=/20060524/APN/605240776

[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