Department of Homeland Security Daily Open Source Infrastructure Report for 05 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 that on Monday, May 1, Idaho State Police issued 75 tickets to drivers who ignored red flashing lights at railroad crossings during an operation to raise public awareness of the dangers motorists and pedestrians face when trying to cross in front of oncoming trains. (See item 12)
- The Department of Homeland Security has kicked−off the first of five regional hurricane preparedness exercises to test improvements made since last year's hurricane season and to identify areas that require additional coordination before the start of this hurricane season, which officially begins June 1. (See item 32)

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 04, Nuclear Regulatory Commission* — **NRC proposes fine for violations involving radiation exposures.** The Nuclear Regulatory Commission (NRC) staff has proposed a $16,250 civil penalty for Epsilon Products Co. for several violations of agency requirements. The most significant violation by the company involved exposures exceeding regulatory limits to five employees and contractors of the firm who are not radiation workers and are therefore considered members of the public. Last August 27th, Epsilon notified the NRC that a gauge containing radioactive material (cesium−137) had malfunctioned at its Marcus Hook, PA, site,

with its radioactive source failing to retract to the shielded position. The NRC investigated and identified six violations, including failures to: maintain dose rates in unrestricted areas below two millirems in any one hour; perform appropriate radiological surveys in unrestricted and uncontrolled areas; provide appropriate training to authorized users of radioactive materials; conduct adequate physical inspections of the fixed gauge at required six−month interval; and develop and implement procedures to test each gauge. The company has removed the gauge involved from service and is conducting a review of its radiation safety program and recommending the revision and/or development of radiation safety procedures, and is taking steps to ensure that only trained staff members are permitted to use gauges containing radioactive material.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2006/06−0 31i.html

2. *May 04, Reuters* — **Lightning, methane caused Sago Mine blast.** A combination of lightning and methane likely caused the explosion that led to the deaths of 12 West Virginia coal miners at Sago Mine in January, investigators said on Thursday, May 4. Echoing the preliminary findings of mine's owner, International Coal Group, federal and state officials told a public hearing they had ruled out coal dust as the cause and that it was likely an unusually strong lightning strike ignited the highly explosive gas in a sealed area. The federal Mine Safety and Health Administration said it believed methane fueled the explosion that caused the deadliest mining disaster in West Virginia since 1968. Investigators found significant circumstantial evidence that lightning caused the explosion, said Monte Hieb of the West Virginia office of Miners Health Safety and Training. He cited a very large lightning strike, one of three near the mine at the time of the explosion, and said the electrical charge could have been transmitted into the mine via utility lines, a belts structure or wire roof mesh.
Source: http://today.reuters.com/news/articlenews.aspx?type=domestic News&storyid=2006−05−04T174340Z_01_N04272711_RTRUKOC_0_US−MI NERALS−SAGO.xml

3. *May 03, Reuters* — **Wind industry giant invests in U.S.** Spain’s Iberdrola, the largest renewable energy operator in the world, has signed deals to buy a U.S. wind power company for $30 million and to study setting up a new wind farm in northern China as it expands abroad to meet its targets. Iberdrola said on Tuesday, May 2, it would buy Pennsylvania−based Community Energy, which has projects to develop 2,200 megawatts (MW) of wind−power capacity along the east coast of the U.S. −− which it described as one of its most important markets. About 200 MW of the capacity are in advanced stages of development while the other 2,000 MW are in preliminary stages and are likely to be approved, Iberdrola said.
Source: http://www.msnbc.msn.com/id/12613761/

4. *May 03, China Daily* — **Emergency system key to nuclear safety.** China has established an emergency response system to nuclear accidents to ensure that the country's nuclear power production program grows safely, the National Atomic Energy Authority said. Such a system at the national, provincial/municipal, and power plant levels has operated well for the past 20 years, the Xinhua News Agency reported. The system is a result of continuing efforts to improve regulations as well as infrastructure related to nuclear power generation, the agency said. The State Council approved a medium− and long−term nuclear power development plan (2006−20) in March, which said nuclear power is a strategic energy source and should be developed to meet the country's growing energy demand. Plans have also been formulated to

help prevent nuclear accidents, Xinhua said. Since China built its first nuclear power plant in 1991, nine nuclear power generation units are now in operation, with a combined capacity of seven million kilowatts. Another nuclear power plant in Tianwan will start operation soon, which will increase the total capacity to 9 million kilowatts. The nation plans to increase the total capacity of its nuclear power plants to 40 million kilowatts by 2020, Xinhua said.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpq%5F%5BhgenrrrTSge%216C%29bfel%5Dv

5. *May 03, U.S. Department of State* — **U.S. nuclear power industry sees expansion in near future.** U.S. energy companies, supported by the Bush administration, are pressing ahead with an ambitious plan for revival of nuclear power, says Steve Kerekes, a spokesperson for the Nuclear Energy Institute (NEI). With nuclear plants running at 90 percent capacity and demand for energy rising, the industry needs to build new plants to keep up or increase its 20 percent share of the electricity market, he said. New orders for nuclear plants would be a sign of a turnaround for the U.S. industry, which has stagnated mostly due to factors beyond its control −− licensing and construction delays, high interest rates on capital, varying plant designs, low natural gas prices, and public opposition to nuclear energy, according to Andrew Paterson of the Department of Energy. For the past 25 years, the industry has added no new plants and focused instead on improving efficiency and safety and increasing production at the existing 103 plants. But in recent years, conditions have changed, Paterson said, including inexpensive and readily available uranium in Canada and Australia, and there are fewer reactor designs and nuclear companies, making planning and running plants easier.
Source: http://usinfo.state.gov/usinfo/Archive/2006/May/03−212802.ht ml?chanlid=washfile

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

6. *May 04, Washington Technology* — **Net−enabled command program moving ahead.** The Defense Information Systems Agency is moving forward on a program to implement Net−enabled command capabilities (NECC), with a request for information (RFI) due for release shortly. The objective of NECC is to provide a comprehensive suite of information services that will enable warfighters to make better, faster and more coordinated decisions on the battlefield, said Maj. Susan Grosenheider, test and evaluation branch chief for the NECC Joint Program Management Office. “The goal is not to be net−centric; it is to impact the battle space,” Grosenheider said. The RFI, to be published in the Commerce Business Daily in the next few weeks, will announce the opening of the federated development and certification environment for companies to submit their products.
Source: http://www.washingtontechnology.com/news/1_1/defense/28504−1 .html

[Return to top]

Banking and Finance Sector

7. *May 04, Websense Security Labs* — **Phishing Alert: Bethpage Federal Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Bethpage Federal Credit Union, based in New York. 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 =480

8. *April 26, Arizona Wildcat* — **University of Arizona targeted in e−mail phishing scam.** On Thursday, April 20, an e−mail was sent to almost all UA e−mails and said the recipient's DM Federal Credit Union account access had been suspended. The e−mail asked customers to go online to restore their accounts, said Eugene Mejia, University of Arizona Police Department spokesperson. The Center for Computer Information and Technology (CCIT) discovered the e−mails did not originate from DM Federal Credit Union, although they contained logos and identifiers stolen from the company's Website. Abraham Kuo of CCIT Security Incident Response Team said the source of the e−mail was located and the problem was remediated shortly after the e−mails were sent out. The destination Website and sending PC address were blocked for campus computers. A warning on the Arizona e−mail system alerted off−campus users. CCIT received several reports of people giving out personal information after receiving the phishing e−mail. Kuo said phishing scams are common through university e−mail, but said this scam was different in that it was sent to almost every UA e−mail. "It was specifically targeted towards the audience here," he said.
Source: http://wildcat.arizona.edu/home/index.cfm?event=displayArticlePrinterFriendly&uStory_id=7c9d0b59−f3df−40f0−81c2−fbc1244f 72c5

[Return to top]

Transportation and Border Security Sector

9. *May 04, USA TODAY* — **Airlines packed in more fliers last month.** New performance reports from airlines suggest that jetliners in the U.S. flew fuller last month than in any April in history. And the early results from April, which indicate that more than 80 percent of U.S. airlines' seats were filled with paying passengers, portend a record−setting −− and uncomfortably crowded −− summer travel season ahead. Seven airlines that have reported for April all show fuller planes. Even discounters Southwest and AirTran, which normally record load factors lower than the big network carriers, came close to filling 80 percent of their April seats. Filing such a high percentage of available seats system−wide means that flights on the most popular routes at the most convenient times were likely to be flying full. For all of 2005, the domestic airline industry filled 77.6 percent of its seats, according to the Air Transport Association. The April numbers are good news for an industry that has lost more than $40 billion over the last five years. Better yet for the industry, travelers have been paying on average about 13 percent more for their tickets than last summer.
Source: http://www.usatoday.com/travel/flights/2006−05−03−airloads−u sat_x.htm

10. *May 04, Journal Register (IL)* — **Spending plan to add Amtrak trains in Illinois.** A proposed $12 million boost in state funding for Amtrak would add passenger trains across Illinois but create logistical challenges for the railroad. Amtrak, which has faced equipment shortages in its national network, may need to find more rail stock for the new service. Also, Amtrak would have to negotiate with the private freight railroads that own the tracks it uses. Spokespeople for three freight railroads −− the Union Pacific, BNSF Railway and CN −− said the companies are trying to determine how to accommodate more Amtrak trains on their busy Illinois lines. Amtrak pays to use the tracks. The Illinois Department of Transportation currently pays Amtrak $12.1 million per year to run passenger trains downstate and from Chicago to Milwaukee. The state−supported trains are different from the federally assisted, long−distance Amtrak trains that also stop in Illinois cities. Under the budget, IDOT's contract with Amtrak would more than double to $24.3 million.
Source: http://www.sj−r.com/sections/news/stories/85172.asp

11. *May 04, Sunday Times (Australia)* — **Man jumps from plane at take off.** An American man allegedly opened a plane door and jumped on to the tarmac after becoming frightened as the aircraft prepared to take off from a New South Wales airport on Thursday, May 4. The 33−year−old man was on the Regional Express (Rex) flight from Merimbula, on the NSW south coast, to Melbourne, when he became alarmed after the cabin was secured and the right engine started, the airline said. The aircraft's pilot saw the man on the ground and immediately aborted takeoff, while airport staff held the man and calmed him until police arrived, Rex officials said in a statement. He was taken to to a local hospital to be assessed and was then questioned by police. A police spokeswoman said the man was later released and the incident was now a matter for the Civil Aviation Safety Authority. No crewmembers or passengers were hurt in the incident and no damage was done to the plane.
Source: http://www.sundaytimes.news.com.au/common/story_page/0,7034,19022926%255E421,00.html

12. *May 04, Associated Press* — **Idaho police catch drivers dodging trains at crossings.** On Monday, May 1, a police officer inside a railroad locomotive working with officers in chase cars issued 75 tickets to drivers who ignored red flashing lights at railroad crossings. Ed Gygli, a captain with the Idaho State Police, said on Wednesday, May 3, that a video camera mounted on the locomotive captured several close calls. Drivers who received a ticket during Monday's "Officer on a Train" operation face a fine of $62. Idaho law requires that drivers stop when red lights start flashing at railroad crossings. The operation was designed to raise public awareness of the dangers motorists and pedestrians face when trying to cross in front of oncoming trains.
Source: http://www.casperstartribune.net/articles/2006/05/03/news/regional/a9b541f34633076e87257163007c2357.txt

13. *May 04, Washington Post* — **Videotaping sparks warning of possible terror surveillance.** Two incidents of "suspicious videotaping" of a European mass−transit system this year prompted a U.S. government warning to domestic homeland security officials Tuesday, May 2, about possible terrorist surveillance. The unclassified Department of Homeland Security "public−sector notice" did not describe the incidents or where they occurred, but said they took place in the past 120 days. The bulletin said the episodes provided "indications of continued terrorist interest in mass−transit systems as targets and potentially useful insight into terrorist

surveillance techniques." The notice was sent to states, domestic law enforcement, and freight and passenger rail carriers. It said that, separately, a foreign national detained last November used a hand−held video camera to film several stations, two line routes, and the interior and exterior of a subway car. "There is not specific or credible intelligence at this time suggesting a threat to U.S.−based mass−transit systems," said Russ Knocke, spokesperson for the Homeland Security Department. "We regularly share information with our homeland security advisers and law enforcement partners . . . to continue to encourage vigilance."
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/05/03/AR2006050302150.html

14. *May 03, Department of Transportation* — **DOT strengthens its proposal for international investment in U.S. airlines.** A revised international investment proposal released on Wednesday, May 3, by the Department of Transportation (DOT) would strengthen requirements initially proposed last November concerning U.S. citizens, control of all safety, security and national defense obligations of domestic airlines while allowing international investors to make decisions on commercial matters involving U.S. airline management. The supplemental notice of proposed rulemaking issued by DOT reflects comments provided on the November 2005 proposal from consumers, airlines, aviation personnel, and other interested groups. That proposal would make it easier for U.S. airlines to raise money, restructure their businesses and form strategic partnerships and alliances by allowing international investors more say in some aspects of airline operations such as scheduling and marketing. The supplemental proposal issued on Wednesday, May 3, would make clear that U.S. citizens who are members of a domestic airline,s board or the voting shareholders, must retain the authority to revoke decision−making authority that international investors may acquire. In addition, the revised proposal would strengthen the original proposal's requirement that U.S. citizens have full control over all policies and implementation relating to safety, security and national defense airlift commitments.
The notice and previous public comment: http://dms.dot.gov docket OST−03−15759.
Source: http://www.dot.gov/affairs/dot5406.htm

[Return to top]

Postal and Shipping Sector

15. *May 04, Associated Press* — **'Forever' stamp would lock rate.** The Postal Service is proposing a "forever" stamp for letters, good no matter how much postal rates increase. The commission has proposed raising the price of a stamp for a letter by three cents, to 42 cents. If the increase takes effect, the forever stamp would be made available for 42 cents. If the first−class rate rises to 45 cents, the 42−cent forever stamp would still be honored on letters. Once the new price took effect, forever stamps would then sell for 45 cents.
Source: http://www.nytimes.com/2006/05/04/washington/04stamp.html?_r =1&oref=slogin

[Return to top]

Agriculture Sector

16. *May 04, USAgNet* — **Arkansas plans for farm database and new mobile emergency command center.** Arkansas agriculture officials are set to launch a $100,000 marketing campaign to urge farmers to register with the government to keep track of dangerous animal sicknesses like mad−cow disease. In addition, the state plans to use federal money to hire two new workers and buy a mobile emergency command center to prepare for avian influenza.
Source: http://www.usagnet.com/story−national.cfm?Id=811&yr=2006

17. *May 04, Integrated Regional Information Networks* — **Jordan: Poultry farmers averse to culling domestic birds.** A Jordanian government campaign against avian flu has been hampered by some citizens' reluctance to cull their homebred birds, health officials said. "Although inspectors from the concerned authorities have tried to convince citizens to get rid of homebred poultry, there are still those who raise various kinds of birds in their backyards," said Khalid Abu Rumman, spokesperson for a government committee tasked with avian flu prevention. Because chicken breeding often represents farmers' sole source of income, many poultry farmers have expressed reluctance to cull their birds en masse. The ministries of agriculture and health, therefore, have proposed poultry vaccinations as a possible alternative to culling.
Source: http://www.irinnews.org/report.asp?ReportID=53146&SelectRegion=Middle_East&SelectCountry=JORDAN

18. *May 04, Reuters* — **Ivory Coast confirms bird flu, boosts controls.** Tests at a reference laboratory have confirmed the deadly H5N1 bird flu in Ivory Coast, triggering extra control measures in the sixth African country hit by the virus, Ivorian animal health authorities said on Thursday, May 4. Bakary Cisse, head of Ivory Coast's epidemiological animal health surveillance network told Reuters that tests by the World Organization for Animal Health laboratory in Padua, Italy, had confirmed birds in the main city, Abidjan, had contracted the virus. Poultry sales will be banned within a radius of two miles of the sites where H5N1 had been confirmed, he added.
Source: http://www.alertnet.org/thenews/newsdesk/L04407133.htm

19. *May 03, Ag Professional* — **More stillbirths in sows if oxytocin is misused.** A main concern of swine producers today is how they can minimize dystocia, or birthing difficulty, and increase the number of piglets born and weaned from a sow. Dystocia can result in an increase in stillbirths, said Mike Tokach, swine scientist for Kansas State University Research and Extension. An increase in stillbirths decreases the number of piglets weaned from a sow. To help ease the birth process and reduce the number of stillbirths, many swine producers administer a hormone called oxytocin, which occurs naturally in gilts and sows. "There is a tendency to overuse oxytocin because producers think it will speed up the farrowing process," Tokach said. "But, really, it's causing the sow to have contractions before piglets are ready [to be born]. This causes ruptured umbilical cords, which results in oxygen deprivation."
Source: http://www.agprofessional.com/show_story.php?id=40161

20. *May 03, Namibian (Africa)* — **Namibia bans Botswana meat imports after confirmed foot−and−mouth disease outbreak.** Namibia has banned imports of meat and live animals from Botswana after the neighboring country confirmed an outbreak of foot−and−mouth disease Tuesday, May 2. Although Namibia does not import meat from Botswana, travelers often bring in animals, meat and meat products into the country from Botswana for their

personal consumption and use. Botswana notified Namibia Tuesday morning of the contagious disease in an eastern town called Selibe−Phikwe. The disease was found in cattle in that area and the town has since been placed under quarantine to restrict the movement of animals.
Source: http://www.namibian.com.na/2006/May/national/061EE542E9.html

21. *May 03, Reuters* — **USDA readies bird flu pandemic plan.** If a bird flu pandemic breaks out, the U.S. Department of Agriculture (USDA) could stagger work shifts and close down day−care centers to help keep operations running, the department's coordinator said on Wednesday, May 3. But he acknowledged there are no guarantees that key functions, including meat inspections and grain shipments, would not be crippled. "What we're trying to plan for is a worst case scenario and have the plan in place," said Peter Thomas, USDA's human pandemic coordinator, told Reuters in an interview. As part of government−wide effort to prepare for a flu outbreak, the USDA has devised its own emergency plan to cover programs and services involving 100,000 employees in nearly 30,000 facilities. It expects to release final details in June.
USDA's role in the Implementation Plan for that National Strategy for Pandemic Influenza: http://www.usda.gov/documents/AI_Fact_Sheet_Implementation_P lan.pdf
White House Fact Sheet: Advancing the Nation's Preparedness for Pandemic Influenza: http://www.whitehouse.gov/infocus/pandemicflu/
Source: http://today.reuters.com/news/articlenews.aspx?type=healthNe ws&storyid=2006−05−04T122344Z_01_N03263343_RTRUKOC_0_US−BIRD FLU−USDA.xml

[Return to top]

Food Sector

22. *May 04, Food Production Daily (Europe)* — **Bacteriophage production begins in Netherlands.** A Netherlands−based company will begin producing bacteria that can be used to kill pathogens in meat and cheese products. With the increasing emphasis by consumers and regulators on food safety, and the prospect of costly recalls, fines and brand damage, processors are constantly on the lookout for quicker and cheaper ways of preventing bacterial contamination of their products. The facility will harbor the Western world's first facility for industrial scale production, the company claimed. The site will also serve as the company's research and development headquarters. In July the company plans to ship its first batches of bacteriophages to customers in the European Union and U.S. The product can be used to control Listeria monocytogenes in cheese and meat products. The company plans to move on to the commercial production of phages for Salmonella, then Campylobacter and other food pathogens.
Source: http://www.foodproductiondaily.com/news/ng.asp?n=67464−ebi−f ood−safety−bacteriophages−listeria

23. *May 04, WRAL (NC)* — **North Carolina police investigate suspected food−tampering at grocery store.** Nearly two weeks ago, workers at a Raleigh, NC, Food Lion noticed a man acting suspicious in the meat section of the store. "It appeared the subject may have pierced a package of meat or torn into a package of meat and had some type of syringe in his hand," said Raleigh police spokesperson Jim Sughrue. On Wednesday, May 3, police arrested Charone

Ladame Josey and charged him with damage to personal property. The meat was immediately removed from store shelves and was turned over to police for testing.
Source: http://www.wral.com/news/9156221/detail.html

24. *May 03, Ag Professional* — **New Japanese drug−residue limits put U.S. pork producers on alert.** The Japanese Ministry of Health, Labor and Welfare will implement new maximum residue limits for veterinary drugs in food including pork and pork products on Monday, May 29, according to a news release from the National Pork Board this week. Producers selling pork to packers exporting to Japan are expected to be able to satisfy these requirements but should take steps to find out if changes to their production practices are required.
National Pork Board news release:
http://www.pork.org/NewsAndInformation/News/News%20Releases/NewsEdit.aspx?NewsID=536
Japan's maximum residue limits for pork: http://www.pork.org/producers/JapanMRL.aspx
Source: http://www.agprofessional.com/show_story.php?id=40163

[Return to top]

Water Sector

25. *May 03, KGPE−TV (CA)* — **Corcoran water not safe to drink yet.** The warning is still in effect for residents of Corcoran, CA −− it's still not safe to drink the water. Health inspectors are testing tap water after city authorities traced contamination to a city well. Residents started noticing dark, sandy water coming out of their taps on Monday, May 1. Showering and hand−washing with the water is safe, but the residents are being reminded not to drink or cook with the tap water until it’s deemed safe again.
Source: http://www.cbs47.tv/news/local/story.aspx?content_id=C1ABBEF5−A779−4B31−8CA7−BE3CA901A0C2

26. *May 02, News Blaze (CA)* — **Space−age drinking water system tested.** U.S. soldiers assigned to the 401st Civil Affairs Battalion in Dahuk, Iraq, have found an alternative way for residents to drink clean water in the village of Bendaway. A polluted creek running through a small village in northern Iraq is the only natural source of drinking water for the residents who live there. Thus, the soldiers are testing a space−age portable water filtering and purification system that was originally designed for NASA, and is modeled after the space shuttle water recycling system.
Source: http://newsblaze.com/story/20060502115728tsop.nb/newsblaze/TOPSTORY/Top−Story.html

[Return to top]

Public Health Sector

27. *May 04, Reuters* — **Genetics might explain why some people get bird flu.** People who have been infected with the H5N1 bird flu virus might be especially susceptible to avian viruses because they are genetically predisposed to them, leading disease experts suggested on

Thursday, May 4. Of the 205 reported cases of human infections since late 2003, there have been many family clusters involving blood relatives, such as father and children, mothers, and daughters. "There have been family clusters. So there has to be certainly a genetic aspect to it," Robert Webster of the St Jude Children's Research Hospital told a bird flu conference organized by the Lancet medical journal in Singapore. Another leading expert Hiroshi Kida, of Hokkaido University in Japan, has long harbored the same theory. "There has not been a single case of infection involving husband and wife," Kida said. Kida is now trying to look for H5N1 survivors in Vietnam and Thailand to verify his theory, and if it proves to be true, it could mean that most people simply cannot catch H5N1 easily −− unless the virus mutates.
Source: http://today.reuters.com/news/articlenews.aspx?type=healthNews&storyid=2006−05−04T122516Z_01_HKG287398_RTRUKOC_0_US−BIRDFLU−GENETICS.xml

28. *May 04, Reuters* — **Bausch confirms eye infection cases in Europe.** Bausch & Lomb Inc. confirmed that its ReNu with MoistureLoc contact−lens solution has been linked to a "handful" of eye infection cases in Europe, the Wall Street Journal reported Thursday, May 4. Bausch spokesperson Margaret Graham did not specify where or how many cases are known. The U.S. Centers for Disease Control and Prevention released a report that suggested an outbreak of Fusarium keratitis, a rare fungal infection that can lead to blindness and potential eye loss, related to its products, may be more widespread than first thought. Cases have already been identified in Asia and the U.S., where the company has pulled its ReNu with MoistureLoc product off store shelves.
Bausch & Lomb Website: http://www.bausch.com/us/vision/concerns/fusarium.jsp
Source: http://news.yahoo.com/s/nm/20060504/hl_nm/bauschandlomb_dc;_ylt=AgLiTBDTR9bNoyW4i3Y7TFIQ.3QA;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

29. *May 04, Associated Press* — **Unsterilized instruments cause hospital HIV scare.** A hospital nurse who failed to clean surgical instruments may have exposed nearly 300 patients to hepatitis or HIV, officials said Wednesday, May 3. Officials at Scripps Memorial Hospital in San Diego said the patients, who all underwent stomach−reduction surgery, had a "very low" risk of infection because the tools had undergone preliminary washes and rinses, although they were not sterilized with chemicals. The nurse knowingly violated operating room procedures when she failed to fully clean a gastroscope, which is used to retrieve other surgical instruments from the stomach, said Scripps spokesman Don Stanziano. The nurse worked at the hospital from September 2004 until last month, when she resigned after hospital officials confronted her. State health officials are investigating the case.
Source: http://www.cnn.com/2006/HEALTH/05/04/dirty.surgery.ap/index. html

30. *May 04, Marketwatch* — **HHS awards for $1 billion flu vaccine R&D.** The Department of Health and Human Services (HHS) awarded a total of $1 billion in research contracts to drugmakers on Thursday, May 4, as part of the government's effort to encourage development of quicker and more efficient modes of vaccine production in case of an avian flu pandemic. According to HHS, the funds are targeted at encouraging cell−based vaccine culturing technologies. According to MedImmune chief executive officer David Mott, cell−based vaccine production could cut down the cultivation time for flu vaccines to as little as three months from the current standard of six to nine months. Mott added that the new techniques can produce

higher yields than older modes, resulting in a greater numbers of doses. He said MedImmune's goal, for example, is to be able to produce 150 million doses within six months of a pandemic being declared. Another issue confronting the vaccine industry has been "drift," which refers to how much a virus mutates over time. A vaccine produced from a batch of virus collected in April, for example, may not be as effective in November because the virus has mutated over that period of time.
Source: http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfinder&siteid=google&guid=%7B2149D99B−78B1−4B76−B196−97B2C13E6DE7%7D&keyword=

31. *May 03, Reno Gazette−Journal (NV)* — **Line break leaves hospital without water.** A second waterline break in two days left Carson Tahoe Regional Medical Center in Carson City, NV, without its water supply Tuesday, May 2, for drinking, bathing, cooking and toilets, officials said. Bottled water, large water jugs and portable toilets were brought in for patients and staff, medical center spokeswoman Diane Rush said. Patients needing emergency operations were being sent to a separate surgery center nearby or to Reno if needed, she said. Officials suspect shifting ground caused by cold and warm outdoor temperatures as a potential cause for the waterline problems. When repairs finish, water tests are needed, Rush said. Service is expected to return in phases.
Source: http://news.rgj.com/apps/pbcs.dll/article?AID=/20060503/NEWS15/605030352/1010/NEWS07

[Return to top]

Government Sector

32. *May 04, Department of Homeland Security* — **DHS drills for 2006 hurricane season.** The Department of Homeland Security has kicked−off the first of five regional hurricane preparedness exercises to test improvements made since last year’s hurricane season and to identify areas that require additional coordination before the start of this hurricane season, which officially begins June 1. The table−top exercises will focus on several key preparedness and disaster response functions, including evacuations, sheltering, National Response Plan implementation, and National Incident Management System activation. The Preparedness Directorate’s Office of Grants and Training developed the exercises with FEMA to engage officials from states and territories in the likely hurricane impact zone. The exercises will include partners at all levels of government, as well as tribal entities, non−governmental organizations and private industry.
Exercise Schedule:
* May 3−4, in Philadelphia, involving Pennsylvania, Virginia, Maryland, Delaware, and the District of Columbia.
* May 8−9 in San Juan, Puerto Rico, involving Puerto Rico and the U.S. Virgin Islands
* May 17−18 in New Orleans, involving Louisiana and Arkansas
* May 31−June 1 in Atlanta, involving Alabama, Florida, Georgia, Kentucky, Mississippi, Tennessee, North Carolina, and South Carolina
* June 20−21 (location TBD), involving New York, New Jersey, Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont
For more information on the exercises, please visit http://www.dhs.gov/hpe

Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0904.xml

[Return to top]

Emergency Services Sector

33. *May 04, Government Accountability Office* — **GAO−06−714T: Hurricane Katrina: Improving Federal Contracting Practices in Disaster Recovery Operations (Testimony).** The devastation experienced throughout the Gulf Coast region in the wake of Hurricanes Katrina and Rita has called into question the government's ability to effectively respond to such disasters. The government needs to understand what went right and what went wrong, and to apply these lessons to strengthen its disaster response and recovery operations. The federal government relies on partnerships across the public and private sectors to achieve critical results in preparing for and responding to natural disasters, with an increasing reliance on contractors to carry out specific aspects of its missions. This testimony discusses how three agencies—the General Services Administration, the Federal Emergency Management Agency (FEMA), and the U.S. Army Corps of Engineers (the Corps)—conducted oversight of 13 key contracts awarded to 12 contractors for hurricane response, as well as public and private sector practices the Government Accountability Office (GAO) identified that provide examples of how the federal government could better manage its disaster−related procurements. While GAO is not making any new recommendations in this testimony, GAO highlights previous recommendations for improving federal procurement in contingency operations.
Highlights: http://www.gao.gov/highlights/d06714thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−714T

34. *May 03, Tampa Bay Newspapers (FL)* — **Florida's barrier islands prepare for storm season.** Evacuations of the barrier islands in Florida are ordered for all hurricanes due to flooding potential, making emergency preparedness in these areas especially critical. Charlie Fant, fire chief of the city of Treasure Island, said that that city is currently undergoing a revision and update of emergency operations. A key part of the city's hurricane preparedness efforts was establishment of an off−island alternate emergency operations center in 2004. Madeira fire Chief Derryl O'Neal heads up that city's disaster management team, which also covers the Redingtons. O'Neal said the disaster plan for the area is now being updated. A big part of the community's emergency planning will be a three−day disaster drill for all city departments being held May 16 to 18. City employees will meet every morning with Chief O'Neal and department heads to learn what is expected of each person and who will be doing what in case a disaster strikes. The drill activity takes the involved employees through the conditions of an actual disaster and the response of emergency personnel. Should a major storm or other calamity occur, everyone involved knows their role and how to respond, O'Neal said.
Source: http://www.tbnweekly.com/content_articles/050306_fpg−03.txt

35. *May 03, Indianapolis Star (IN)* — **Mock disaster in Indiana will test emergency agencies.** The Johnson County Emergency Management Agency (EMA) in New Whiteland, IN, is organizing a mock disaster for Saturday, May 6. The drill's disaster will be a mock terrorism event. "It will involve a crop−dusting plane spraying chemicals over the school and then followed by a second chemical attack," said Forrest Sutton, the county EMA director. The magnitude of the "attack" will be large enough to test the entire Central Indiana Emergency

Management System's ability to react. A private vendor will evaluate the agencies' responses.
Source: http://www.indystar.com/apps/pbcs.dll/article?AID=/20060503/LOCAL04/605030325/−1/ZONES04

36. *May 02, Chicago Sun−Times* — **New digital radios to link Chicago's first responders.** In Illinois, communication breakdowns could be a thing of the past thanks to a no−bid $22 million digital radio system on the way for Chicago's first responders. Police officers and firefighters will be able to communicate directly with each other, instead of relying on the cumbersome process of "console patching" by 911 center dispatchers. Firefighters and paramedics will use the same hand−held radios, instead of being forced to carry two different radios if they want to communicate directly. The system −− complete with more than 2,000 portable radios for the Chicago Fire Department alone −− will also have more frequencies to handle heavy traffic volumes during major emergencies. Some channels will be "encrypted" for enhanced security. And the new digital system will be able to maintain uninterrupted communication in high−rise buildings where radio service is notoriously difficult. "It's a big step in fire communications −− the biggest upgrade that's been undertaken in at least 25 years," said fire department spokesman Larry Langford.
Source: http://www.suntimes.com/output/news/cst−nws−radio02.html

[Return to top]

Information Technology and Telecommunications Sector

37. *May 04, Associated Press* — **Spammer identifies 'do not spam' addresses.** One spammer has managed to identify e−mail addresses on Blue Security's Blue Frog "do−not−spam" list, taking advantage of an obvious flaw with such lists and prompting critics to wonder what took so long. The lists are generally encrypted so spammers can't mine them for new addresses. However, John Levine, co−author of Fighting Spam for Dummies, said spammers merely have to run their lists, see what's been removed and compare that with the original to find out the addresses on the "do−not−spam" lists.
Source: http://www.smh.com.au/news/breaking/spammer−identifies−do−not−spam−addresses/2006/05/04/1146335837392.html

38. *May 03, Security Focus* — **Mozilla Firefox iframe.content window.focus deleted object reference vulnerability.** Mozilla Firefox is prone to a vulnerability when rendering malformed JavaScript content. An attacker could exploit this issue to cause the browser to fail or potentially execute arbitrary code. Analysis: The memory corruption error when processing a specially crafted HTML script that contains references to deleted objects and the "designMode" property is enabled, which could be exploited by attackers to crash a vulnerable browser or remotely take complete control of an affected system by tricking a user into visiting a malicious Webpage.
Vulnerable: Mozilla Firefox 1.5.2; Mozilla Firefox 1.5.1; Mozilla Firefox 1.5 beta 2; Mozilla Firefox 1.5 beta 1; Mozilla Firefox 1.5; Mozilla Firefox 1.5.0.2.
Not vulnerable: Mozilla Firefox 1.5.3.
Solution: The vendor has released an advisory, along with fixes to address this issue. Please see the referenced advisory for further information:
http://www.mozilla.org/security/announce/2006/mfsa2006−30.ht ml

Source: http://www.securityfocus.com/bid/17671/discuss

39. *May 03, Sophos* — **Russian student convicted for running virus distribution Websites.** Sophos has reported the sentencing of a man who not only created his own malware, but ran two Websites distributing over 4000 different computer viruses. Sergey Kazachkov, a Russian science university student from Voronezh, was found guilty of making available thousands of pieces of malware via two virus exchange Websites. He was also said to have created and spread his own malicious software. Kazachkov has been given a two year suspended sentence, and will have to abide by conditions laid down by the court during a one year probation period.
Source: http://www.sophos.com/pressoffice/news/articles/2006/05/russ ianvx.html

40. *May 03, Tech Web* — **Massive DoS attack knocks TypePad, LiveJournal blogs offline.** Millions of blogs hosted by LiveJournal and TypePad were unavailable throughout Tuesday night, May 2, and into Wednesday morning, May 3, as a massive denial−of−service attack struck their servers. The attack that brought down the servers at Six Apart −− the San Francisco company behind the LiveJournal and TypePad services, and the Moveable Type blogging software −− began at 4 p.m. PDT Tuesday, according to an advisory posted to the firm's Website by Michael Sippey, the vice president of product. According to Sippey, service was interrupted for the following: TypePad, LiveJournal, TypeKey, sixapart.com, movabletype.org and movabletype.com.
Source: http://www.techweb.com/wire/security/187200053

41. *May 03, Silicon* — **Apple online store hacked.** Apple Computer's Korean online store has been defaced by an intruder. The attack was apparently carried out by someone working under the name "Dinam," who claimed in his online posting to be Turkish. The defacement was removed from Apple's Website.
Source: http://networks.silicon.com/webwatch/0,39024667,39158606,00. htm

42. *May 03, Register (UK)* — **Hackers libel Canadian prime minister on train signs.** Bewildered Toronto, Canada, train passengers were left scratching their heads after a hacker altered advertising signs in order to mock Stephen Harper, the country's prime minister, on the westbound Lakeshore GO Transit train. Scrolling LED signs on several trains repeated the message "Stephen Harper Eats Babies" every three seconds during the duration of the attack. Security specialists told the Toronto Star that the attack was probably carried out by a remote control device that can be used to program scrolling electronic signs. The kit can be bought over the counter at electronic hobby stores, such as Sam's Club.
Source: http://www.theregister.co.uk/2006/05/03/canadian_train_sign_ hack/

43. *May 02, SecuriTeam* — **Vulnerability issues in implementations of the Domain Name System protocol.** The vulnerabilities described in this advisory affect implementations of the Domain Name System protocol. Many vendors include support for this protocol in their products and may be impacted to varying degrees, if at all. Analysis: If exploited, these vulnerabilities could cause a variety of outcomes including, for example, a denial−of−service condition. In most cases, they can expose memory corruption, stack corruption or other types of fatal error conditions. Some of these conditions may expose the protocol to typical buffer overflow exploits, allowing arbitrary code to execute or the system to be modified. The following vendors have provided information about how their products are affected by this

vulnerability: Cisco Systems, Inc MyDNS; Delegate pdnsd; Ethereal Sun; Hitachi Wind River; ISC; Juniper Networks; Microsoft. Refer to source advisory for further detail on vendor vulnerabilities.
Source: http://www.securiteam.com/securitynews/5IP020KIKU.html

44. *May 02, SecuriTeam* — **Multiple vulnerabilities in Linux−based Cisco products.** A vulnerability in the CiscoWorks WLSE "show" CLI application allows execution of arbitrary code as the root user. Analysis: The Cisco shell presents the administrator with a restricted set of commands which includes a "show" application. The "show" application has several vulnerabilities which allow an attacker to "break out" of the shell and execute commands (including /bin/sh) as the root user. A cross site scripting flaw exists in: /wlse/configure/archive/archiveApplyDisplay.jsp with the "displayMsg" parameter. This can be used to steal the JSP session cookie, therefore giving a targeted attacker admin level access to the system. Once the attacker has admin Web GUI access to the system via the XSS, they can then change the admin password or create a new admin user (without requiring the admin password).
Affected software: Cisco Wireless Lan Solution Engine (WLSE); Cisco Hosting Solution Engine (HSE); Cisco Ethernet Subscriber Solution Engine (ESSE); Cisco User Registration Tool (URT); CiscoWorks2000 Service Management Solution (SMS); Cisco Vlan Policy Server (VPS); Cisco Management Engine (ME1100 Series); CiscoWorks Service Level Manager (SLM).
Solution: Cisco has released patches for the vulnerabilities.
Cisco Security Advisory: http://www.cisco.com/warp/public/707/cisco−sa−20060419−wlse.shtml
Cisco Security Response: http://www.cisco.com/warp/public/707/cisco−sr−20060419−priv.shtml
Source: http://www.securiteam.com/unixfocus/5LP050KIKW.html

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 releases 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), 25 (smtp), 445 (microsoft−ds), 32459 (−−−), 50497 (−−−), 32777 (sometimes−rpc17), 2728 (sqdr), 20482 (−−−) 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

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov 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