Department of Homeland Security Daily Open Source Infrastructure Report for 30 May 2007

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 six Florida customs inspectors have told federal officials that superiors instructed them to enter false data indicating airline passengers had been stopped and inspected for plant and animal contraband. (See item 16)
- The Los Angeles Daily News reports due to a creeping chemical plume threatening the water supply, the Department of Water and Power has shut down at least one drinking−water well in Los Angeles because of contamination of the San Fernando Valley aquifer, with the possibility that the contamination will spread. (See item 22)
- The University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism has made its terrorism attack database publicly available, providing a unique service for understanding risk in the context of terrorism threats. (See item 29)

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 29, Bloomberg* — **Colorado, Utah rival OPEC reserves, lure Chevron, Exxon, Shell.** Colorado and Utah have as much oil as Saudi Arabia, Iran, Iraq, Venezuela, Nigeria, Kuwait, Libya, Angola, Algeria, Indonesia, Qatar and the United Arab Emirates combined. Trapped in

limestone up to 200 feet thick in the two Rocky Mountain states is enough so−called shale oil to rival that of the Organization of the Petroleum Exporting Countries (OPEC) and supply the U.S. for a century. Exxon Mobil, Chevron, and Royal Dutch Shell are spending $100 million a year testing new methods to separate the oil from the stone for as little as $30 a barrel. Industry executives and analysts say new technology and persistently high prices make the idea feasible. "The breakthrough is that now the oil companies have a way of getting this oil out of the ground without the massive energy and manpower costs that killed these projects in the 1970s," said Pete Stark of IHS Inc. "All the shale rocks in the world are going to be revisited now to see how much oil they contain."
Source: http://www.bloomberg.com/apps/news?pid=20601103&sid=aoZ7q9LhDrVs&refer=news

2. *May 29, Washington Post* — **China embraces nuclear future.** As governments worldwide look at nuclear power as a possible answer to global warming, China has embarked on a nuclear−plant construction binge that eventually could exceed the one the United States undertook during the technology's heyday in the 1960s. Under plans already announced, China intends to spend $50 billion to build 32 nuclear plants by 2020. Some analysts say the country will build 300 more by the middle of the century. That's not much less than the generating power of all the nuclear plants in the world today. By that point, the Chinese economy is expected to be the world's largest, and the idea that it may get most of its electricity from nuclear fission is being met with both optimism and concern. China's plans already have been felt in world markets. Chinese Premier Wen Jiabao has been traveling the world to secure contracts for the uranium needed to power nuclear reactors, striking deals recently with Australia and Niger. Higher worldwide demand and a fear of future shortages have driven the price of processed uranium ore from $10 a pound in 2003 to $120 this month.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/05/28/AR2007052801051.html

3. *May 28, Courier Press (IN)* — **New law to help thwart metal theft.** Thieves stealing copper wire and metal pipe to sell for scrap have become such a problem that the Indiana Legislature has passed a new state law to help police solve the crimes. Construction sites and utility substations are the targets most often hit, police say. Suspected thieves are fencing the stolen metal by selling it for scrap. Even if police catch up with the stolen items at a scrap yard, the scrap dealer might not have a record of the transaction. The new state law, House Bill 1324, requires scrap metal recyclers to keep additional records or logs of customers selling copper, aluminum, brass or other valuable metals used in residential or commercial construction. Police can inspect the records at any time. State Representative Dave Crooks, who authored the bill said meeting the records requirement could be as basic as scrap dealers photocopying the customer's driver's license and sales receipt and keeping them in a manila folder. Crooks authored the bill after rural electric cooperatives expressed concern about thefts of copper wire from utilities. The law takes effect July 1.
Source: http://www.courierpress.com/news/2007/may/28/new−law−to−help−thwart−metal−theft/

4. *May 28, Chicago Tribune* — **Safety focus tightens after refinery blast.** Outside Gate 1 of the second−largest oil refinery in the U.S., a block−lettered sign carries a seemingly simple message: "What You Say Leads to Action." Sloganeering signs do not a culture make, but the

placard at least puts in writing what the people running BP's Texas City refinery are trying to accomplish. To Robert Malone, who was brought in as president of BP America after a series of mishaps that started with Texas City and wound up with 200,000 gallons spilled on the Arctic tundra in Alaska, the job of updating BP's refineries is tied tightly to the effort to change the corporate culture. One example: At any refinery, one of the most dangerous periods comes when equipment comes back on line. Malone is trying to change BP's culture to make the process safer. The Texas City refinery explosion occurred during a restart after repairs. Now, no equipment comes back on line at BP without a thorough safety check backed up with signed assurances that procedures have been followed. Supervisors also must now be present. Every worker has the right to stop the restart process, no questions asked, if anything seems amiss.
Source: http://www.chicagotribune.com/news/nationworld/chi−mon_bp_sidemay28,1,604051.story?coll=chi−newsnationworld−hed

5. *May 27, Government Security News* — **DHS to study planned sites for nuke facilities.** The Nuclear Regulatory Commission (NRC) and the Department of Homeland Security (DHS) have signed a Memorandum of Understanding, under which DHS will review "potential vulnerabilities" of any site being considered for a nuclear facility. The agreement, signed last month, is designed to enhance the security of all future nuclear plant sites. According to a report of the Memorandum, published by the NRC in the Federal Register, the agreement "establishes a process to implement provisions of the Energy Policy Act." The agreement specifically states: "Before issuing a license for a utilization facility [commercial nuclear power plant], the NRC shall consult with DHS concerning the potential vulnerabilities of the location of the proposed facility to terrorist attack." Under the terms of the agreement, NRC would consult DHS experts prior to approving any particular site. DHS experts would in turn evaluate all sites under consideration, assessing the impact of the following factors: Pedestrian and vehicular land approaches; Railroad approaches; Waterborne approaches; Potential "high−ground" adversary advantage areas; Nearby road and/or transportation routes; Nearby hazardous materials facilities, airports, dams, military and chemical facilities and pipelines.
Source: http://www.gsnmagazine.com/may_07/nuke_facilities.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *May 29, Ventura County Star (CA)* — **Ammonia leak prompts road closure.** About 180 employees of an onion processing plant in Oxnard, CA, were evacuated and one required medical care Monday night, May 28, after an ammonia leak. A plant supervisor who detected the leak was taken to the hospital, but he was in the process of being released Monday night. The other employees were taken to a building near the plant. Authorities said there was no danger to the surrounding area. The incident resulted in the closure of Mountain View Avenue from Richmond Avenue on the west to Rose Avenue on the east, and the closure of Pacific Avenue from Fifth Street on the north to Wooley Road on the south.
Source: http://www.venturacountystar.com/news/2007/may/29/180−workers−evacuated−1−hurt−in−ammonia−leak/

7. *May 27, Associated Press* — **Metal plating plant explosion kills one.** Authorities say a boiler explosion at a metal plating plant in Chester County, PA, critically injured three workers, one

of whom later died. The three workers suffered serious burns Saturday, May 26, in the blast at the melt shop at Mittal Steel, formerly I−S−G Plate, in the old Lukens Steel complex in South Coatesville. Two men were flown to the burn unit at Crozer−Chester Medical Center, where a hospital official says one died during the night.
Source: http://abclocal.go.com/wpvi/story?section=local&id=5343795

8. *May 25, San Francisco Chronicle* — **A hundred residents asked to remain indoors following chlorine gas leak.** An advisory for Pittsburg, CA, residents who live near the Calpine power plant to stay indoors was lifted Friday, May 25. People in more than 100 Pittsburg homes were asked to stay inside Thursday morning, as a precaution after a chlorine gas leak at the Calpine plant on East Third Street. Three Calpine workers were taken to the hospital after they apparently inhaled some of the gas. Randy Sawyer, director for the county's hazardous materials program, said workers at the plant accidentally mixed acid with bleach, creating chlorine. Officials believe they created about 600 pounds of chlorine. Officials said the county activated its telephone notification system to warn residents in about 106 homes north of the plant, near the Antioch border.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/c/a/2007/05/25/BABADIGEST2.DTL&feed=rss.bayarea

[Return to top]

Defense Industrial Base Sector

9. *May 28, Washington Times* — **China intent on aircraft carrier goal.** The new commander of U.S. military forces in the Pacific and Asia says he found Chinese military leaders intensely interested in acquiring aircraft carriers during a recent visit to that country. Adm. Timothy J. Keating added in an interview that he had warned the Chinese about the huge challenges involved in building and manning an aircraft carrier. "I suggested let's not be naive about the complexity of those ships, and they are not cheap," he said. The admiral, a naval aviator who has made 1,200 carrier landings, said all of the Chinese leaders with whom he spoke during a five−day stay this month indicated their inclination to pursue the development of aircraft carriers. Chinese ambitions to acquire aircraft carriers were described last week in a Pentagon report titled, "Military Power of the People's Republic of China 2007."
Pentagon report: http://www.defenselink.mil/pubs/pdfs/070523−China−Military−Power−final.pdf
Source: http://washingtontimes.com/world/20070527−115808−1213r.htm

[Return to top]

Banking and Finance Sector

10. *May 29, SC Magazine* — **Kiwibank target of phishing scam.** An e−mail purporting to be from New Zealand’s Kiwibank −− urging customers to update their personal information −− is a malicious phishing campaign, warns Sophos. Using the Kiwibank logo, the e−mail tricks customers into clicking on the provided link in order to update their personal information and ensure their eligibility for the bank’s policy if guaranteeing their money. According to Paul

Ducklin, head of technology, APAC at Sophos the Website appears to be a legitimate Website. The site is now blocklisted and off the air and the genuine owner of the site is left to sort out the mess. "SophosLabs currently estimates that 70 percent of malicious Web pages abused by phishers and malware spreaders are not directly associated with cybercriminals, but rather are legitimate sites which have been broken into and 'borrowed' for criminal activity," said Ducklin.
Source: http://www.itnews.com.au/newsstory.aspx?CIaNID=53062&src=sit e−marq

11. *May 29, Department of the Treasury* — **Treasury designation targets Sudanese government, rebel leader.** The U.S. Department of the Treasury Tuesday, May 29, blocked the assets of three Sudanese individuals, including two high−ranking government officials and a rebel leader, for their roles in fomenting violence and human rights abuses in Darfur. The Treasury also acted to sanction 30 Sudanese companies owned or controlled by the Government of Sudan, and one company that has violated the arms embargo in Darfur. Ahmad Muhammed Harun, Sudan's State Minister for Humanitarian Affairs, has been accused of war crimes in Darfur by the International Criminal Court in The Hague. Sudan's head of Military Intelligence and Security, Awad Ibn Auf, was also designated, along with Khalil Ibrahim, leader of the Justice and Equality Movement. The action brings to seven the number of Sudanese individuals for whom access to the U.S. financial system is prohibited under Executive Order 13400, which targets perpetrators of human rights abuses in Darfur in western Sudan. An additional 30 companies have been designated on Tuesday pursuant to Executive Orders 13067 and 13412 because they are owned or controlled by the Government of Sudan.
Complete list of individuals and entities designated Tuesday:
http://www.treasury.gov/offices/enforcement/ofac/actions/200 70529.shtml .
Source: http://www.treasury.gov/press/releases/hp426.htm

12. *May 28, Inquirer (PA)* — **VA: Doctors' data threatened by theft.** The Department of Veterans Affairs (VA) is warning more than 1.3 million doctors across the nation this month that their personal prescribing information may have been stolen in the loss of an external computer hard drive from the VA Medical Center in Birmingham, AL. The department says it believes the hard drive contained billing information from 1.3 million doctors and the Social Security numbers and other personal data from 199,000 patients. The Iomega hard drive was reported missing January 22. Veterans received notification letters in March, and local doctors are just now receiving letters. Jo Schuda, a VA spokesperson in Washington, said doctors' and patients' names were taken from Medicare and Medicaid, the federal health programs, as part of a quality assessment study, and "everyone who treats a veteran at some point is included in the database." The loss of the hard drive was the second incident in the last year. A VA laptop computer and disks containing personal information from 26.5 million veterans were stolen last May but were recovered a month later.
Source: http://www.philly.com/inquirer/magazine/20070528_VA__Doctors_data_threatened_by_theft.html

13. *May 28, SecurityFocus* — **BBB Trojan nabs more than 1,400 victims.** An e−mail attack that dresses itself up as a complaint filed with the Better Business Bureau (BBB) has infected the computers of more than 1,400 executives, according to an analysis published by SecurityFocus. The phishing attack uses details apparently culled from public sources to tailor the e−mail message with a company's name, the name of a senior executive and the executive's e−mail

address in an attempt to convince the person to open an attachment. There appears to be two variants of the Trojan horse program, one that uses a browser helper object to collect all information that passes through the victim's browser and another that uses a more traditional keylogger, according to SecureWorks' Joe Stewart. Stewart found that the first variant had collected information on the online activities of more than 1,400 business executives, totaling more than 145 Mbytes of data. "Most phishing/keylogger schemes we see are not targeted...In contrast, the BBB phishing Trojan attempts to collect all interactive data sent out from the Web browsers of a small set, relatively speaking, of very high−value targets," says Stewart.
Source: http://www.securityfocus.com/brief/511

[Return to top]

Transportation and Border Security Sector

14. *May 29, CheapFlights (MA)* — **Inline luggage system makes Midway faster, less crowded.** A new $42−million inline baggage handling system recently replaced nine bulky, lobby−located explosive detection systems (EDS) in the north half of the ticketing lobby at Midway Airport in Chicago. Now, checked luggage bound for the bellies of airplanes is screened behind−the−scenes on a conveyor system. The inline set−up is designed to process as many as 4,500 pieces of luggage per hour. If it performs up to specs, that will make it three times faster than the previous stand−alone EDS set−up. Inline systems are also touted as less labor intensive. That means Transportation Security Administration officers can be better deployed around airports, at security checkpoints on in training. The south half will get the same system in July.
Source: http://news.cheapflights.com/airlines/2007/05/inline_luggage__1.html

15. *May 28, Associated Press* — **Lightning strikes JetBlue plane with 140 passengers going to JFK.** An airplane carrying 140 passengers was struck by lightning Sunday evening, May 27, and made an emergency landing, but no one was hurt. The JetBlue Airways Airbus A320 was heading from Rochester to New York's John F. Kennedy International Airport (JFK) when the lightning hit it, causing a smell similar to that of an electrical fire to enter the passenger cabin, company spokesperson Bryan Baldwin said. There was no fire or smoke, he said. The emergency, which allowed Flight 43 to land at the Queens airport before other scheduled flights, meant the passengers got to their destination about 20 minutes early, Baldwin said.
Source: http://www.usatoday.com/weather/storms/2007−05−28−jetblue−li ghtning_N.htm

16. *May 26, Associated Press* — **Florida customs workers report falsifying data.** Six customs inspectors have told federal officials that superiors instructed them to enter false data indicating airline passengers had been stopped and inspected for plant and animal contraband. The U.S. Customs and Border Protection officers allege that in 2005, supervisors at Orlando Sanford International Airport told them to falsify information typically gathered during direct interviews and inspections of international passengers or crewmembers, according to a report by the U.S. Office of Special Counsel. The six officers were agricultural specialists, employed to detect and stop introduction of animal and plant pests into the United States. The inspectors told the Special Counsel's office that they were instructed to enter the false data because the airport was busy. The whistle−blowers allege that when questioned about the practice, supervisors said that "things were done differently in Sanford." One agent entered the information without ever

receiving any security clearance or training, according to the Special Counsel's office documents.
Source: http://www.usatoday.com/travel/flights/2007−05−26−florida−cu stoms_N.htm

17. *May 25, Government Computer News* — **DHS: Additional SBINet wireless test will teach lessons.** The Department of Homeland Security (DHS) will start a second wireless test of its Border Net project in the Great Lakes region of the United States. Rod MacDonald, the Customs and Border Protection (CBP) Directorate's assistant commissioner, said May 21, that the program will build on lessons learned in an Arizona pilot test, which examined how different devices connected to the directorate's database through assorted wireless connections. "The Arizona pilot was pretty successful," MacDonald said during a panel discussion at the Homeland Security Science and Technology Stakeholders Conference in Washington. MacDonald said that because the Secure Border Initiative network (SBInet) will focus on the southern border first, testing the technologies on the northern border lets CBP explore different environments and get out ahead of a multibillion−dollar program. MacDonald said he didn't know exactly when the northern border test would begin, but it should happen this summer. The Border Net test showed how border agents could connect to CBP's database through notebook PCs and personal digital assistants through technologies such as WiMax, cellular, Wi−Fi and Mesh.
Source: http://www.gcn.com/online/vol1_no1/44342−1.html

18. *May 25, Department of Transportation* — **Traffic deaths on America's highways down slightly, but too many lives are still lost.** Department of Transportation Secretary Mary E. Peters on Friday, May 25, announced that traffic deaths on U.S. roads were down slightly in 2006 according to preliminary figures, but cautioned that far too many lives continue to be lost. While the number of road deaths is projected to have declined slightly nationwide from 43,443 in 2005 to 43,300 in 2006, "even one death is too many," Secretary Peters said. And over half of passenger vehicle occupants killed died unbuckled, the preliminary data shows. The Secretary noted that, as the summer driving season starts, police officers around the country will be on patrol looking for people who aren't buckling up. She added that the Department supports states with millions of dollars in highway safety funds annually, including the nearly $27 million being used to support seat belt enforcement efforts. The final 2006 report, pending completion of data collection and analysis, will be available in late summer.
The preliminary report: http://www−nrd.nhtsa.dot.gov/Pubs/810755.PDF
Source: http://www.dot.gov/affairs/dot5307.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

Nothing to report.

[Return to top]

Food Sector

19. *May 28, Yonhap News (South Korea)* — **South Korea to mull lifting ban on U.S. bone−in beef.** South Korea will engage in talks that could result in the lifting of its ban on U.S. bone−in beef following Washington's official request for the revision of import safety and quarantine rules, the government said Monday, May 28. In a news conference, Finance and Economy Minister Kwon O−kyu and Agriculture Minister Park Hong−soo said Seoul respects a recommendation made by the World Organization for Animal Health (OIE) last week in Paris. "We intend to engage in earnest talks on the import rule revision issue in accordance with internationally set standards and scientific procedures," the finance minister said. He said Seoul plans to conduct its own independent risk assessment analysis, and that talks with the U.S. could be concluded around September if there are no unforeseen complications. The new classification technically allows the U.S. to sell most beef products, including ribs, without restrictions. South Korea, however, has the right to decide on its own import conditions.
Source: http://english.yonhapnews.co.kr/Engnews/20070528/64000000002 0070528175450E2.html

20. *May 27, Associated Press* — **Nicaragua seizes Chinese−made toothpaste.** Nicaraguan police seized 6,000 tubes of a Chinese−made toothpaste suspected of containing a chemical that killed at least 51 people in Panama last year, the health minister said Sunday, May 27. All U.S. imports of Chinese toothpaste were halted last week to test for diethylene glycol −− a chemical commonly used in antifreeze and brake fluid. Nicaraguan Health Minister Maritza Cuan said the toothpaste had been smuggled in from Panama. The product also could have been smuggled from Panama to Honduras and Colombia. Panama ordered the toothpaste pulled from shelves there earlier this month after finding it contained diethylene glycol. At least 51 people died in Panama since October after taking medicine contaminated with diethylene glycol. The substance was found in cough syrup and other medications made in a Panama government laboratory from a falsely labeled shipment that workers thought was glycerin. The chemical was traced to a Chinese company.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/05 /27/AR2007052700652.html

21. *May 25, Bloomberg News* — **Sesame butter recalled.** Whole Foods Market Inc., the largest U.S. natural−foods grocer, is recalling sesame seed butter over possible contamination with salmonella. No confirmed illnesses have been reported so far, Whole Foods said in a statement. The voluntary recall is for a Whole Foods store brand of tahini, a form of ground sesame used in Middle Eastern dishes.
Source: http://www.chicagotribune.com/business/chi−070525wholefoods− recall−story,0,2797778.story?coll=chi−bizfront−hed

[Return to top]

Water Sector

22. *May 27, Los Angeles Daily News* — **Los Angeles water wells threatened.** More than four years after being warned that a creeping chemical plume was threatening Los Angeles, CA's water supply, the Department of Water and Power (DWP) has shut down at least one drinking−water well because of contamination of the San Fernando Valley aquifer. The North Hollywood well closure means that, for the first time, Los Angeles will be unable to draw its full allotment of groundwater, forcing it to import water at a cost of $7.3 million. But more troubling than the cost, DWP officials say, is the possibility that the contamination will spread and ruin Los Angeles' only local water supply −− the San Fernando Valley underground reservoir that can serve residents in an emergency. Los Angeles imports 85 percent of its drinking water from the Sierra Nevada Mountains and Colorado River, with the San Fernando Valley groundwater basin supplying the rest. And in dry years the city can draw as much as 30 percent of its supply from the groundwater, saving on the cost of importing more water. This year, however, the spreading contamination means the city will be able to draw only 10 percent of its supply from local groundwater.
Source: http://www.dailynews.com/news/ci_5997595

[Return to top]

Public Health Sector

23. *May 28, New York Times* — **Outbreak of eye infections puzzles officials.** Health officials and eye doctors are puzzled by an outbreak of a rare but potentially blinding eye infection that led the manufacturer of a contact lens cleaning solution to withdraw one of its products. The outbreak resembles one last year that was linked to a different manufacturer's lens solution and a different microbe. In both instances, the cornea, the eye's transparent outer covering, is at risk. But why two different microbes caused the outbreaks is not known. Acanthamoeba keratitis is caused by a parasite, can be difficult to detect and is hard to treat. This outbreak has involved at least 138 patients. Last year, an outbreak of fusarium keratitis was caused by a fungus; there were 164 confirmed cases. It was linked to ReNu With MoistureLoc made by Bausch & Lomb, but how the product caused the problem is unknown. Epidemiologists from the U.S. Centers for Disease Control and Prevention have linked the acanthamoeba keratitis outbreak to AMO Complete Moisture Plus Multi−Purpose Solution. Advanced Medical Optics of Santa Ana, Calif., manufactures the solution, which is used to clean and store soft contact lenses.
Source: http://www.nytimes.com/2007/05/28/us/28eyes.html?_r=2&hp&oref=slogin&oref=slogin

24. *May 28, Boston Globe* — **Avian flu proves a persistent foe.** Avian flu continues to strike in certain corners of the world. So far this year, at least 44 people have contracted the disease, mainly in Indonesia and Egypt. Three of every five people contracting avian flu this year have died. For more than four years, disease trackers have monitored the movement of avian flu from Asia to the Middle East and then into Africa and the edge of Europe. Its ability to kill with such frequency ignited fears that the virus, known as H5N1, could spark a global flu epidemic capable of claiming millions of lives. In most cases, health authorities have determined that the human victims of the virus contracted it directly from infected birds. And while there is no indication that the virus has acquired the ability to spread easily human−to−human, disease specialists said its persistent presence is evidence that it remains a threat. The H5N1 virus now

causing trouble was identified in Hong Kong in 1997 and then vanished −− at least among humans −− until 2003, when three people in Vietnam and one in China contracted the disease. They all died. In the next three years, 259 more people fell ill from avian flu; 154 of them died.
Source: http://www.boston.com/yourlife/health/diseases/articles/2007/05/28/as_deadly_as_ever_avian_flu_proves_a_persistent_foe/

25. *May 28, Archives on Internal Medicine* — **Community−associated methicillin−resistant Staphylococcus aureus skin and soft tissue infections at a public hospital.** At a 464−bed public hospital in Chicago, IL, and its more than 100 associated clinics, surveillance of soft tissue, abscess fluid, joint fluid, and bone cultures for S aureus was performed. The incidence of Community−associated methicillin−resistant Staphylococcus aureus (CA−MRSA) skin and soft tissue infections increased from 24 cases per 100,000 people in 2000 to 164.2 cases per 100,000 people in 2005 (relative risk, 6.84 [2005 vs 2000]). Risk factors were incarceration (odds ratio [OR], 1.92; 95 percent confidence interval [CI], 1.00−3.67), African American race/ethnicity (OR, 1.91; 95 percent CI, 1.28−2.87), and residence at a group of geographically proximate public housing complexes (OR, 2.50; 95 percent CI, 1.25−4.98); older age was inversely related (OR, 0.89; 95 percent CI, 0.82−0.96 [for each decade increase]). Of 73 strains tested, 79 percent were pulsed−field gel electrophoresis type USA300. CA−MRSA infection has emerged among Chicago's urban poor. It has occurred in addition to, not in place of, methicillin−susceptible S aureus infection.
Source: http://archinte.ama−assn.org/cgi/content/short/167/10/1026

26. *May 28, PLoS Medicine* — **Prophylactic and therapeutic efficacy of human monoclonal antibodies against H5N1 influenza.** New prophylactic and therapeutic strategies to combat human infections with highly pathogenic avian influenza (HPAI) H5N1 viruses are needed. Using Epstein−Barr virus researchers immortalized memory B cells from Vietnamese adults who had recovered from infections with HPAI H5N1 viruses. Supernatants from B cell lines were screened in a virus neutralization assay. B cell lines secreting neutralizing antibodies were cloned and the mAbs purified. The cross−reactivity of these antibodies for different strains of H5N1 was tested in vitro by neutralization assays, and their prophylactic and therapeutic efficacy in vivo was tested in mice. In vitro, mAbs FLA3.14 and FLD20.19 neutralized both Clade I and Clade II H5N1 viruses, whilst FLA5.10 and FLD21.140 neutralized Clade I viruses only. In vivo, FLA3.14 and FLA5.10 conferred protection from lethality in mice challenged with A/Vietnam/1203/04 (H5N1) in a dose−dependent manner. mAb prophylaxis provided a statistically significant reduction in pulmonary virus titer, reduced associated inflammation in the lungs, and restricted extrapulmonary dissemination of the virus. Therapeutic doses of FLA3.14, FLA5.10, FLD20.19, and FLD21.140 provided robust protection from lethality at least up to 72 h postinfection with A/Vietnam/1203/04 (H5N1). A panel of neutralizing, cross−reactive mAbs might be useful for prophylaxis or adjunctive treatment of human cases of H5N1 influenza.
Source: http://medicine.plosjournals.org/perlserv/?request=get−document&doi=10.1371/journal.pmed.0040178

27. *May 27, Agence France−Presse* — **Nearly 100 people hospitalized with encephalitis in China.** Nearly 100 people have been sent to hospital after an outbreak of encephalitis B in southwest China, state media said Sunday, May 27. More than 30 of the patients were being treated at Shidian county hospital in Baoshan, a city in Yunnan province near the border with

Myanmar, the Xinhua news agency reported. The hospital has received more than 40 encephalitis B patients over the past week, later allowing some with milder cases to return home. Dozens of others were treated at other hospitals. Encephalitis causes inflammation of the membranes around the brain. Death may result as the inflamed tissue is squeezed against the inside of the skull. Reported cases of encephalitis B are rare in China. In the latest monthly report on infectious diseases from the health ministry, just one case was recorded in April.
Source: http://news.yahoo.com/s/afp/20070527/hl_afp/healthchinadisease_070527221234;_ylt=ApbSHVW16LvuCQA54A9d9jSJOrgF

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

28. *May 28, Press of Atlantic City (NJ)* — **Text messages could be life−saver in emergency.** A hurricane can cut off electricity and shut down roads. Lingering storms can make it impossible to call relatives. But the same technology that teenagers use to text message could help emergency responders continue to communicate, a state researcher says. Elizabeth Gomez, an information specialist, said that during disasters and heavy weather, cell−phone signals could degrade to the point that speech is not possible. “But there's nearly always enough signal to send text,” Gomez said. That is because texting works in quick bursts and requires significantly less signal to send. But even though a text message can get through, Gomez said, digital space and time are limited. “You have to know how to shrink your dialogue to 160 characters,” she said. “That's the architecture of text messaging on the phone.” “The most important thing is knowing what to say in a crisis,” Gomez said. Gomez said speak plainly and get to the point.
Source: http://www.pressofatlanticcity.com/top_three/story/7481826p−7376794c.html

29. *May 28, Homeland Security Watch* — **University of Maryland terror database should inform risk analysis.** The University of Maryland’s National Consortium for the Study of Terrorism and Responses to Terrorism (START) made its terrorism attack database publicly available. It provides a unique service for understanding the big picture, but other uses may include adding depth to the challenge of understanding risk in the context of terrorism threats. With content covering about 80,000 incidents between 1970 and 2004, it provides one of the few data sources for risk analysis of this scope and detail. Intentional attacks disallow a conventional approach to gauging risk because data points (incidents) are the result of adaptive causes (perpetrators). Because factors other than frequency and severity should inform assessments of terrorism risk, it is noteworthy that the START database includes 45 factors that can be used to determine antecedent markers, common vulnerabilities, and other trends of that emerge from a deep look at past cases. While trend setting is one way of judging risk, another is just plain insight and anticipation of likely events, outcomes, and relevant impact based on good information.
Source: http://www.hlswatch.com/2007/05/28/umd−terror−database−now−p

ublic−should−inform−risk−analysis/

[Return to top]

Information Technology and Telecommunications Sector

30. *May 29, Chicago Tribune* — **Attacks on Estonia move to new front.** After Estonia relocated a Soviet war memorial out of downtown Tallinn last month, furious Russians rioted in the Estonian capital, tried to attack Estonia's ambassador in Moscow, and hastily engineered de facto economic sanctions against the tiny Baltic nation. But the salvo from the Russian side that has most worried Estonians is a carefully crafted three−week cyber attack on Estonian government, bank and media Websites that has wreaked havoc in a country heavily dependent on the Internet for everything from banking and voting to paying taxes. The onslaught of "denial−of−service" attacks, many of which have originated from Russian computers, has raised questions about whether such attacks will become a tactic in future political conflicts. U.S. Deputy Secretary of State John Negroponte said the cyber sabotage in Estonia should prompt countries to shore up defenses against hackers and cyber−terrorists. Hackers routinely use Internet−connected computers as a conduit for attacks without the owner's knowledge. And Estonian officials have yet to prove that the Russian government instigated the sabotage.
Source: http://www.chicagotribune.com/technology/chi−estonia_rodriguezmay29,1,6793241.story?coll=chi−techtopheds−hed

31. *May 28, Computerworld* — **Mac OS open to attack through unpatched Samba.** Hackers can attack Apple Inc.'s Mac OS X by exploiting an unpatched vulnerability in the open−source Samba file−and print−sharing software that's included with the operating system, Symantec Inc. said Monday, May 28. Samba is enabled when Mac users turn on the Windows Sharing feature that allows Microsoft Corp. customers to access files and printers on a Mac network. Symantec was able to exploit "the heap corruption vulnerability on a fully patched Mac OS X 10.4.9 system running the default Samba 3.0.10 application." Although Mac OS X doesn't turn on Samba by default, Macs that share a network with Windows PCs could be at risk, Symantec warned. Because Apple has not released a Samba update since 2005, users must upgrade to the latest, and secure version, themselves.
Samba Website: http://us4.samba.org/samba/
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9021518&intsrc=hm_list

32. *May 28, SecurityFocus* — **Peer−to−peer networks co−opted for DOS attacks.** A flaw in the design of a popular peer−to−peer network software has given attackers the ability to create massive denial−of−service attacks that can easily overwhelm corporate Websites, a security firm warned last week. Over the past three months, more than 40 companies have endured attacks emanating from hundreds of thousands of Internet protocol addresses (IPs), with many of the attacks producing more than a gigabit of junk data every second, according to security solutions provider Prolexic Technologies. The latest attacks came from a collection of computers running peer−to−peer software known as DC++. The software is based on Direct Connect, a protocol which allows the exchange of files between instant messaging clients. The directories of where to find certain files resides in a few servers, known as hubs. Older versions of the hub server software have a flaw that allows an attacker to direct clients to get information

from another server, said Fredrik Ullner, a developer for the DC++ project. Maliciously redirecting those client results in a large number of computers continuously demanding data from the victim's Web server, overwhelming it with requests.
Source: http://www.securityfocus.com/news/11466

Internet Alert Dashboard

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

33. *May 29, Associated Press* — **Private guards a weak link in security.** Legions of ill−trained, low−paid private security guards are protecting tempting terrorist targets across the U.S. The security guard industry found itself involuntarily transformed after September 2001 from an army of "rent−a−cops" to protectors of the homeland. Yet many security officers are paid little more than restaurant cooks or janitors. The industry is governed by a maze of conflicting state rules, according to a nationwide survey by The Associated Press. Wide chasms exist among states in requirements for training and background checks. Tens of thousands of guard applicants were found to have criminal backgrounds. Paul Maniscalco, a senior research scientist at George Washington University, is helping to change the security guard culture. He recently developed an anti−terrorism computer course for shopping mall guards, who are being taught that they now have more concerns than rowdy teenagers and shoplifters. Congressional investigators reported last year that 89 private guards working at two military bases had histories that included assault, larceny, possession and use of controlled substances and forgery. The security businesses' own trade group, representing the largest firms, acknowledges the industry as a whole isn't ready to recognize signs of terrorism and respond to an attack.
Source: http://us.rd.yahoo.com/dailynews/ap/brand/SIG=br2v03;_ylt=AmgAQi9nF7cKLuH6HOFnWsKWwvIE/*http://www.ap.org

34. *May 23, Government Accountability Office* — **GAO−07−908R: U.S. Army Corps of Engineers' Procurement of Pumping Systems for the New Orleans Drainage Canals (Correspondence).** The Corps' decisions to acquire the 34 hydraulic pumping systems were focused on satisfying its commitment to have pumping capacity on the drainage canals in place by June 1, 2006 −− the start of the 2006 hurricane season. In order to increase the likelihood that pumping capacity would be in place when needed, the Corps utilized several tools to expedite and streamline the acquisition process. The Corps appears to have had a valid reason for each of the iterative decisions it made at each stage of the procurement process. The cumulative effect of these decisions resulted in one supplier −− Moving Water Industries Corporation −− being in the strongest competitive position to receive the contract for the pumping systems. Since June 1, 2006, the Corps has continued to take steps to correct known performance problems with the pumping systems, including uninstalling them to make some

repairs. Specific problems that have been addressed include replacing some components that were undersized, such as springs and motors; re−welding of some critical structural welds; and revising certain start−up procedures. However, the total planned pumping capacity will still not meet the Sewerage and Water Board's drainage needs to keep the city from flooding during a hurricane when the canal gates are closed.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−908R

[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