Department of Homeland Security Daily Open Source Infrastructure Report for 31 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 a security guard at the Three Mile Island nuclear power plant in Dauphin County, Pennsylvania, was so absorbed in playing a hand−held video game that he failed to see an inspector approach during a surprise inspection. (See item 2)
- NBC reports seventy passengers on an Amtrak train bound for Indiana were made to sit on the train for nearly seven hours after an engineer reportedly disobeyed a traffic signal and had to undergo a drug test. (See item 20)
- Reuters reports the World Health Organization has issued a pandemic influenza draft protocol for rapid response and containment −− a step−by−step plan for containing a bird flu outbreak if the virus starts to spread rapidly among humans. (See item 30)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *May 30, Providence Journal (RI)* — **Fire crews taxed in electricity plant blaze.** The fire on the roof of the six−story Manchester Street power station in Providence, RI, required all 92 city firefighters working Monday, May 29, to extinguish. Chief David Costa called every working firefighter as well as crews from three neighboring communities to the Manchester Street power

station. The call came in at 4:39 p.m. EDT. The electric power plant, fueled by natural gas, powers much of Rhode Island. The plant is owned by Dominion Resources Inc. The fire was in a metal ventilation shaft that went through the roof, the chief said. The roof around the shaft was also on fire. The cause of blaze was still being investigated. It took about two and a half hours to get the fire under control. Costa said damage was limited mostly to the roof. He estimated $20,000 to $30,000 worth of damage. To his knowledge, there weren't any power outages as a result of the fire, he said.
Source: http://www.projo.com/news/content/projo_20060530_fire30.1289d260.html

2. *May 29, Associated Press* — **Three Mile Island guard playing video game fails to see inspector.** A security guard at the Three Mile Island nuclear power plant was so absorbed in playing a hand−held video game that he failed to see an inspector approach during a surprise inspection, the agency said. The employee did not violate any rules as guards are allowed to engage in mind−stimulating activities, the state Department of Environmental Protection said. But the alleged lapse −− which follows five other reports of employee inattention in the past two years −− is prompting officials to review current policies. Kathleen McGinty, secretary of the environmental agency, said "The real issue is that his complete absorption in the game distracted him from noticing the repeated approach of our inspector. And that shows why this procedure needs to be changed and these video games disallowed," she said. The state agency will work with the U.S. Nuclear Regulatory Commission and nuclear plant operators to review policies after the latest inspection. The department's nuclear safety staff conducted a surprise check between 4 a.m. and 8 a.m. EDT Friday, May 26, at the Dauphin County, PA, plant. The guard did respond properly to a radio check while the inspector was present, McGinty said.
Source: http://www.usatoday.com/tech/gaming/2006−05−29−nuclear−guard−game_x.htm?POE=TECISVA

3. *May 28, Associated Press* — **Massive investment in oil refineries could cut global fuel prices, expert says.** Oil companies and other investors are spending a collective $100 billion on new oil refineries that could alleviate the current bottleneck in refining capacity and eventually translate into a small cut in the price of gasoline, Will Rathvon, global head of project finance for Standard Chartered Bank, said. More than 30 new or expanded refineries will come on stream over the next decade, adding at least 6.5 million barrels a day of badly needed capacity to global fuel markets. "Right now refining is maxed out," Rathvon said on the sidelines of a Middle East energy conference. "At this point, the shutdown of a single refinery even for maintenance can trigger an increase in gasoline prices." Refineries in fuel−thirsty Asia are operating at a frantic 95 percent capacity, Rathvon said. In North America and Europe, refineries are also running at over 90 percent capacity, he said. New refining capacity of at least 6.5 million barrels per day over the next decade could shave two or three dollars from the price of a barrel of crude oil. Americans might see a five to ten cent reduction in the price of a gallon of gasoline, Rathvon said.
Source: http://abcnews.go.com/Business/print?id=2015178

4. *May 27, Associated Press* — **Navajos, Sithe sign lease for power plant in northwest New Mexico.** Navajo Nation officials and Houston−based energy company Sithe Global Power have signed lease agreements that would allow a 1,500−megawatt power plant to be built on tribal land in northwestern New Mexico. The coal−fired Desert Rock Power Plant, when complete, would produce enough electricity to power up to 1.5 million homes. The Navajo Council

approved the 50−year lease on Friday, May 12. It covers a 590−acre site south of Shiprock, NM.
Source: http://www.mohavedailynews.com/articles/2006/05/28/news/stat e/state3.txt

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *May 27, Honolulu Advertiser* — **Chemical leak in Hawaii prompts business evacuations.** A chemical leak in a Lîhue, HI, warehouse Saturday morning, May 27, led to the evacuation of all businesses in Lîhue Industrial Park II. The leak occurred when an employee of Trex Hawaii, LLC was transferring methyltrichlorosilane from a storage tank to a process tank in the company's Aukele Street warehouse. It was determined that the tank sprang a leak due a faulty valve.
Source: http://the.honoluluadvertiser.com/article/2006/May/27/br/br0 6p.html

[Return to top]

Defense Industrial Base Sector

6. *May 29, European Defense Agency* — **Report: European defense research and technology spending is increasing.** The European Defense Agency (EDA) now has accurate data available on what its 24 participating Member States spend on Defense Research and Technology (R&T). The overall level of Defense R&T expenditure is increasing in 2006, as is the amount spent collaboratively. Although the proportion spent collaboratively shows an increase, the vast majority of R&T projects and programs are conducted on a purely national basis. EDA concludes that investing just 1.25 percent of the $232 billion total defense spending in Defense R&T is clearly not enough to sustain Europe’s future technological and industrial base.
The full report: http://www.eda.europa.eu/facts/Defence%20R&T%20Spend.pdf
Source: http://www.eda.europa.eu/facts/Defence%20R&T%20Spend.htm

7. *May 25, Government of the People (China)* — **Chinese government unveils plan for developing defense technology by 2020.** The Chinese government plans to enhance its capability to innovate, develop and rapidly supply new−generation weaponry over the next 15 years under a new national development program. The outline of the development program of science and technology for national defense for 2006 to 2020 was passed by the Commission of Science, Technology and Industry for National Defense at a meeting on Thursday, May 25, in Qingdao, east China's Shandong Province. The outline states that national defense industry will focus on development of: new and high−tech weaponry; high−tech industries for both military and civilian purposes; manufacturing technologies for military industries; basic and frontier technologies for national defense; and guaranteeing technological innovation for national defense. The outline stresses that the country will develop high and new tech weaponry to reinforce a mechanized and information−based army.
Source: http://english.gov.cn/2006−05/25/content_290888.htm

[Return to top]

Banking and Finance Sector

8. *May 30, New York Times* — **Technology and easy credit give identity thieves an edge.** Officials and consumer advocates point to recent trends to extend more credit to more people with fewer hassles, and retailers and consumers embracing instant, near−anonymous access to credit, for the uptick in identity theft. Brad H. Astrowsky, a former prosecutor, said "There's a disconnect between corporate leadership at financial institutions and their security departments...Marketing people...can do things to fix the problem, but they have no incentive and motivation to do it." Arizona is a hot spot for identity theft because Maricopa County is one of the fastest−growing counties in the nation, and its growth exaggerates trends that exist in many communities: a mobile population and high numbers of immigrants and retirees. It has a heavy traffic in methamphetamine, whose users sort through trash for Social Security numbers or bank account numbers. The newest wave of thefts involves using a machine that hotels use to recode room keys to copy the magnetic strip from a victim's credit card onto the back of another.
   Source: http://www.nytimes.com/2006/05/30/us/30identity.html?ei=5088&en=f77c2572cbfb4709&ex=1306641600&partner=rssnyt&emc=rss&pa gewanted=print

9. *May 30, Viruslist.com* — **Password−stealing Trojan arrives in German spam.** Spam with a password−stealing Trojan horse has been detected. It uses a German−language pitch, saying the malicious attachment is an official Microsoft Corp. Windows update.
   Trojan−PSW.Win32.Sinowal.u is part of the Sinowal family of password stealing Trojans which steals usernames and passwords entered via forms in an Internet browser. It particularly targets certain banking domains and also has the ability to steal other locally stored passwords. Sinowal has a special trick: when an infected user visits certain banking domains Sinowal inserts some of its own HTML code into the page. This is done to create a customized pop up which asks the user for personal information.
   Source: http://www.viruslist.com/en/weblog?weblogid=187634800

10. *May 30, Japan Economic Newswire* — **Police arrest alleged member of Yahoo Japan auction phishing ring.** The Kyoto police on Tuesday, May 30, arrested a man suspected of belonging to a phishing ring who stole personal information on people who accessed a fake Yahoo Japan auctions site. It is the first police crackdown in Japan on an organized phishing fraud case, according to the Kyoto police. The police said they have obtained arrest warrants for seven other people in the ring. The Tokyo−based ring is suspected of stealing the personal information of some 1,000 people since last year and to have defrauded some 700 people of about 100 million yen by using the data. From September 2005 to April 2006, the group sent users of the auction service unsolicited e−mails purporting to show their Yahoo auction records, the police said. When recipients clicked on a Web link in the spam they were taken to a fake Yahoo auction site and some of them provided their ID's and passwords, which the group used to access the real auction site and spuriously put items, including watches and audio equipment, up for sale, the police said. People who made what they thought were successful bids on the items wired payments to the group's bank accounts.
    Source: http://www.tmcnet.com/usubmit/−police−arrest−alleged−member−yahoo−japan−auction−phishing−/2006/05/30/1661880.htm

11. *May 30, Associated Press* — **Bush taps Paulson for Secretary of the Department of Treasury.** Department of Treasury Secretary John Snow resigned Tuesday, May 30, and President Bush nominated Goldman Sachs chairman and chief executive officer Henry M. Paulson Jr. as his replacement. The Senate Finance Committee is expected to act swiftly on the nomination. A spokesperson for the panel said it was possible a hearing could be conducted within the next few weeks, depending on how quickly the necessary paperwork for the nomination is supplied to the panel.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/05/30/AR2006053000365_pf.html

12. *May 30, Government Accountability Office* — **GAO−06−386: Bank Secrecy Act: Opportunities Exist for FinCEN and the Banking Regulators to Further Strengthen the Framework for Consistent BSA Oversight (Report).** The U.S. government's framework for preventing, detecting, and prosecuting money laundering has been expanding through additional pieces of legislation since the passage of the Bank Secrecy Act (BSA) in 1970. In recent years, noncompliance with BSA requirements has raised concerns in Congress about the ability of federal banking regulators to oversee compliance at depository institutions and ensure that these institutions have the controls necessary to identify suspicious activity. In light of these concerns, the Government Accountability Office (GAO) was asked to determine how federal banking regulators examine for BSA compliance and identify and track violations to ensure timely corrective action. GAO also was asked to determine how enforcement actions are taken for violations of the BSA. To further strengthen BSA oversight, GAO recommends that FinCEN and the regulators communicate emerging risks through updates of the interagency examination manual and other guidance; periodically review BSA violation data to determine if additional guidance is needed; and, jointly assess the feasibility of developing a uniform classification system for BSA compliance problems. FinCEN and the regulators supported these recommendations and said they are committed to ongoing interagency coordination to address them.
Highlights: http://www.gao.gov/new.items/d06386.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−386

13. *May 29, InfoWorld* — **Phishers use Microsoft Word hole as bait.** Microsoft last week said it would rush to deliver a patch for a recently discovered hole in Microsoft Word that was being used in sophisticated online attacks. The warning came after anti−virus firms reported focused "spear phishing" attacks against companies and government agencies in the European Union and the U.S. that used the Word flaw to plant Trojan horse programs on vulnerable machines. The attacks are rated "low" for most companies. However, that could change if the Word exploit is circulated widely, said Johannes Ullrich of the SANS Internet Storm Center.
Source: http://www.infoworld.com/article/06/05/29/78647_22NNwordspearphish_1.html?source=rss&url=http://www.infoworld.com/article/06/05/29/78647_22NNwordspearphish_1.html

14. *May 29, Times Herald (PA)* — **Warning: New scam.** In a twist on the "Nigerian scams" common to spam e−mails, thieves have begun using telephone services for the deaf to contact businesses. The TDD or TTY services allow deaf people to type comments to a relay center. The service allows scammers to cover poor English or heavy accents, said Det. James Angelucci. Each state is required to provide deaf telephone service. Scammers in Ghana

contacted a Norristown, PA, businessman via e−mail in mid−May with a plan to send furniture to a religious center in Alaska. When he asked to speak to him over the phone, they then used the TDD lines. The scammers told the businessman they found a discount shipper, but the shipper would not take credit cards. Scammers sent the victim a credit card number, and asked for a cash advance to be wired to them in Africa so they could pay the shipping company. AT&T said the callers probably accesses the system using Voice Over Internet Protocol. The victim complied, and lost $1,800 when the credit card company contacted him and told him the card was fraudulent. Other companies have become victims this way. The cases are generally referred to the FBI, Angelucci said.
Source: http://www.timesherald.com/site/news.cfm?newsid=16706575&BRD=1672&PAG=461&dept_id=33380&rfi=6

15. *May 29, Associated Press* — **Man counterfeits Cumberland County, North Carolina, checks.** The latest victim of identity theft: Cumberland County, NC. Edwin Lynwood Reid of Fayetteville, NC, was arrested Friday, May 19, accused of counterfeiting $6,759 in county checks and cashing them at local businesses in April. A local bank discovered the bogus payments and alerted police. Reid also allegedly wrote checks belonging to the Louisiana Treasury Department and Chacco Inc., a heating and air conditioning company in Fayetteville. County officials have kept the case quiet, fearing that if they reveal too many details, others may learn from Reid. While the county provides salaries through electronic deposits, Amy Cannon, the county's finance director, said the county signs about 3,000 checks a month for other transactions. Both the county and its bank, RBC Centura, have safeguards on their checks to protect from counterfeiting, Cannon said.
Source: http://dwb.newsobserver.com/news/ncwire_news/story/2953509p−9391484c.html

16. *May 27, Business Wire* — **Goldleaf Technologies responds to phishing attempt.** Goldleaf Technologies, a provider of Web−based ACH and check conversion solutions, announced Saturday, May 27, that it has identified and responded to attempts to redirect its clients' customers to a phishing Website to entice them to enter their personal financial information. The company had temporarily suspended all Internet access to Goldleaf Technologies' Website services, but the company has corrected the problem and fully restored all services.
Source: http://www.tmcnet.com/usubmit/2006/05/27/1661245.htm

[Return to top]

Transportation and Border Security Sector

17. *May 30, Detroit Free Press (MI)* — **Trimmer Northwest now flies as No. 5.** Northwest Airlines has lost its title as the nation's fourth−largest airline, reflecting the large number of planes and flights it has shed as it reorganizes. The fewer flights mean more crowded seating for passengers and higher prices to destinations where Northwest has little competition. The cutbacks have caused low−cost carriers like Spirit and AirTran to add destinations from Northwest's hubs, including Detroit. Continental Airlines moves into No. 4, based on the number of miles it carries paying passengers. Northwest, which is sharply cutting costs after filing for bankruptcy protection last fall, hopes to emerge as a profitable airline, which could lead to growth, analysts said.
Source: http://www.usatoday.com/travel/flights/2006−05−30−nwa−no5_x. htm

18. *May 30, Associated Press* — **Plane from Los Angeles clips fence as it arrives at JFK airport.** A Qantas Airways airplane arriving at John F. Kennedy International Airport (JFK) from Los Angeles clipped a fence as it taxied after landing, authorities said. No one was hurt, and the plane wasn't significantly damaged. The Qantas plane landed safely Monday, May 29, at about 5:30 p.m. EDT, according to Tony Ciavolella, a spokesperson for the Port Authority of New York and New Jersey, which operates the region's airports. As the plane taxied to a runway, it bumped the fence, Ciavolella said. Qantas Airways Ltd., based in Australia, is investigating the incident, an airline spokesperson said. The plane, Quantas flight 107, was being directed by an "airport marshaller" at the time of the incident, he said.
Source: http://www.nbc4.tv/news/9291395/detail.html

19. *May 30, Reuters* — **EU court rules airline data deal with U.S. illegal.** The European Union (EU) acted illegally when it agreed to transfer airline passenger data to the United States as part of U.S. efforts to fight terrorism, the bloc's highest court said on Tuesday, May 30. The United States, the executive European Commission, and European airlines said the ruling would have no immediate impact on transatlantic air travel and left time to find an agreed solution to the data transfer issue. Under a May 2004 EU−U.S. agreement, European airlines have been obliged to give U.S. authorities 34 items of information on passengers flying to the United States, including name, address, all forms of payment, and contact telephone numbers. The United States insisted the transfer of personal details was essential to fight terrorism following the September 11 attacks. The European Court of Justice ruled that the EU Council of Ministers' decision to sign the agreement lacked an adequate legal basis. It gave the European Commission and member states four months to find a solution by maintaining the legality of the decision to sign the agreement until September 30.
Source: http://www.usatoday.com/travel/news/2006−05−30−eu−passenger− data_x.htm

20. *May 30, NBC5 (IL)* — **Train halted after engineer allegedly runs light.** Seventy passengers on an Amtrak train bound for Indiana were made to sit on the train for nearly seven hours after an engineer reportedly disobeyed a traffic signal and had to undergo a drug test late Sunday, May 28, in south suburban Dolton, IL. Train 318, bound from Chicago to Indianapolis, had left Chicago about 7:45 p.m. CDT and then about 9 p.m., stopped unexpectedly in an intersection near Dolton, according to 22−year−old New Albany, IN, resident Brandon Richie. "We were told that our engineer ran a red light," said Richie, adding that hours went by where no one on the train knew what was happening, and neither customer service for Metra nor local police were very helpful. According to Amtrak spokesperson Vernae Graham, two buses, one an express, arrived to take the passengers to Indianapolis. "The engineer was relieved, meaning he can no longer operate the train," said Graham, who would not comment when asked if he was taken for drug testing because of the alleged violation.
Source: http://www.nbc5.com/travelgetaways/9288238/detail.html

21. *May 29, Washington Technology* — **Surveillance intrusion detection top priorities.** Security doesn’t stop at the water’s surface at the Port of Lake Charles in Louisiana, one of largest liquid natural gas ports in the country. Underwater sonar, radar, and a network of sensors search for threats. The information is charted into a common operational picture that is shared with nearby agencies, including law enforcement, Coast Guard, and immigration officials. As Congress prepares to approve increased funding for port security grants, contractors said the money is

likely to pay for more comprehensive surveillance, domain awareness and information−sharing IT systems which, in many cases, systems integrators are installing. The Department of Homeland Security listed protection against improvised explosive devices as a top goal of its port security grants for 2005, and is expected to do so again for 2006 grant guidance. To guard against such dangers, many ports implement surveillance and intrusion detection systems that are shared with law enforcement. “It’s not gates, guns and guards any more,” said Aaron Ellis, a spokesperson for the American Association of Port Authorities, a trade group for 85 major ports. Recently, focus has been on IT surveillance and communications networks that can offer a common reference point and tools for use among response agencies.
Source: http://www.washingtontechnology.com/news/21_10/federal/28652_−1.html

[Return to top]

Postal and Shipping Sector

22. *May 30, DMNews* — **Washington Mutual, USPS seek to extend suspension on negotiated service agreement.** Washington Mutual Bank and the U.S. Postal Service (USPS) asked the Postal Rate Commission (PRC) for permission to extend their suspension of proceedings on their negotiated service agreement (NSA) until June 2, according to a document filed with the commission May 26. The parties want to review two recent PRC filings regarding other NSAs and revise their own. The postal service had filed for an NSA with Washington Mutual Bank on March 29 based on encouraging the company to increase its use of First Class Mail. The USPS is seeking a three−year deal covering First Class Mail for the bank's credit card services. An NSA is a contract between the USPS and a company, providing customized pricing incentives based on the company's mail operations. Changes in rates and mail classifications needed to implement an NSA require review and recommendation by the PRC and approval by the USPS Board of Governors. Seattle's Washington Mutual provides financial services for consumers and small businesses.
Source: http://www.dmnews.com/cms/dm−news/direct−mail/36912.html

23. *May 27, Courier−Journal (KY)* — **FedEx buys Watkins trucking company.** FedEx Corp. announced on Friday, May 26, it is buying Watkins Motor Lines for $780 million, stepping up its competition with UPS in the ground freight market. Just months ago, UPS announced plans to pay $1.25 billion to buy Overnite Corp., now known as UPS Freight. The deal marked the entry of UPS into the less−than−truckload business. It is the same business in which Watkins also specializes. These carriers combine smaller loads from many customers on one truck and sort them at a central hub −− a system FedEx and UPS are already adept at through their businesses. Watkins, a privately held company in Lakeland, FL, will be renamed FedEx National LTL and operate as a separate network within the FedEx Freight division. Memphis−based FedEx also agreed to acquire the assets of Watkins' business in Canada, Watkins Canada Express, which will be renamed FedEx Freight Canada.
Source: http://www.courier−journal.com/apps/pbcs.dll/article?AID=/20060527/BUSINESS/605270352/1003

[Return to top]

Agriculture Sector

24. *May 30, USAgNet* — **Foot−and−mouth continues to spread in Vietnam.** Foot−and−mouth disease has stricken two more Vietnamese provinces, raising the number of its affected localities to 38, according to a local animal health agency on Thursday, May 25. The new outbreaks with some 80 infected pigs were found in the southern provinces of An Giang and Kien Giang, said the Department of Animal Health under the Ministry of Agriculture and Rural Development. Twelve out of 38 affected localities, including eight northern provinces of Cao Bang, Bac Can, Ha Giang, Thai Nguyen, Phu Tho, Yen Bai, Hai Duong and Lai Chau; two central localities, namely Nghe An province and Da Nang city; and two central highlands provinces of Gia Lai and Lam Dong, had declared foot−and−mouth outbreaks in their territories. The disease has spread to 421 communes in 38 cities and provinces nationwide.
Source: http://www.usagnet.com/story−national.cfm?Id=1018&yr=2006

25. *May 30, San Francisco Chronicle* — **Shortage of veterinarians throughout California.** "We know in California we need 725 or 750 new vet practitioners in the state annually, and we do not come close," said Bennie Osburn, dean of the University of California Davis School of Veterinary Medicine. The Bureau of Labor Statistics projects 28,000 veterinary job openings nationwide by 2012. The nation's 28 veterinary colleges aren't satisfying the demand. The situation is most dire when it comes to those who treat farm animals. In California's countryside, the vet shortage is more than an inconvenience −− it's a problem that some experts fear is depriving farm animals of the care they need, leaving them vulnerable to disease. One shortage is veterinarians trained for government work, such as protecting the food supply and countering epidemics. About half of state and federal veterinarians are nearing or are eligible for retirement, Osburn said.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/c/a/2006/05/30/ BUGF8J3DIF1.DTL

26. *May 30, Chesapeake Bay Journal* — **Tagging program will track mycobacteria's impact on rockfish population.** Mug shots of fish captured from Virginia’s Rappahannock River may provide important clues for scientists trying to resolve one of the Bay’s most perplexing mysteries: What happens to the plethora of sick striped bass swimming in the Chesapeake? Last fall, researchers from the Virginia Institute of Marine Science tagged, extensively photographed, and then released 1,811 fish captured in the river. Some fish seemed healthy, others had the skin lesions that have become common on many rockfish in recent years. As fishermen catch the tagged fish and return them for a $20 reward, scientists can go to their mug shot gallery and determine whether individual stripers seem to be getting worse, or better. And, if sick fish are returned at a lower rate, it would be the most concrete evidence −− after a decade of research −− that mycobacteriosis is killing striped bass in the wild. Mycobacteriosis −− and what it means for the Bay’s most valuable recreational species −− has been scientists and fishery managers since it was discovered in 1997. It is a chronic wasting disease which, in aquaculture, usually results in death. But mortality has been rarely reported in the wild, and scientists are unclear about the disease’s impact on Bay fish.
Source: http://www.bayjournal.com/article.cfm?article=2827

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

27. *May 30, BBC News* — **Pollution risks Yangtze River's death.** The Yangtze, China's longest river, is "cancerous" with pollution, reports in the country's state media have said. Environmental experts fear pollution from untreated agricultural and industrial waste could turn the Yangtze into a "dead river" within five years. That would make it unable to provide drinking water to the booming cities along its banks. The Yangtze rises in China's western mountains and passes through some of its most densely populated areas. The government has promised to clean up the Yangtze, which supplies water to almost 200 cities along its banks. But experts speaking in China's state media say that unless action is taken quickly, billions of tons of untreated industrial and agricultural waste and sewage are likely to kill what remains of the river's plant and wildlife species within five years. China's rapid economic development means that many of the nation's waterways are facing similar problems. Last year the authorities announced that the country's second−longest river, the Yellow River, was so polluted that it was not safe for drinking.
Source: http://news.bbc.co.uk/2/hi/asia−pacific/5029136.stm

[Return to top]

Public Health Sector

28. *May 30, RIA Novosti (Russia)* — **Russia tests human bird flu vaccine.** Trials on humans of a bird flu vaccine have begun in Moscow, a senior doctor said Tuesday, May 30. "We have started tests on 120 volunteers," said Vitaly Zverev, the head of the Mechnikov Vaccine and Serum Research Institute. "They are mainly medical staff, doctors and donors. They are all healthy adults aged between 18 and 45." Tests of the vaccine are also under way at the St. Petersburg−based Influenza Research Institute. The developers of the vaccine said it presented no danger to the volunteers and scientists underlined that the vaccine had been created on the basis of a non−pandemic H5N1 bird flu strain.
Source: http://en.rian.ru/russia/20060530/48804475.html

29. *May 30, Times (United Kingdom)* — **Injured in Indonesia have to wait days at hospitals with five for each bed.** Two days after the earthquake that killed almost 9,000 people on Java, Indonesia, the international aid effort shifted Monday, May 29, from the hunt for buried survivors to the struggle to prevent sickness and hunger among hundreds of thousands of homeless survivors. Despite an influx of doctors from Indonesia and overseas, many of the injured complained that they had waited almost two days for treatment. Hospitals in the affected area have almost five injured patients for every bed, and supplies of drugs and food are dwindling. Between 20,000 and 30,000 are injured, according to the United Nations, and they are choking the region’s hospitals. In Jebugan hospital in the town of Bantul, there were 500 inpatients under treatment Monday, May 29, an improvement on the 1,200 the day before. But

the hospital has only 110 beds and ten full−time doctors.
Source: http://www.timesonline.co.uk/article/0,,3−2202278,00.html

30. *May 30, Reuters* — **World Health Organization issues plan to limit bird flu outbreak in humans.** The World Health Organization (WHO) issued a step−by−step plan on Tuesday, May 30, for containing a bird flu outbreak if the virus starts to spread rapidly among humans. Under the detailed timeline laid down, a country should notify WHO of a cluster of suspicious cases suggesting sustained human−to−human spread of the virus within 24 hours of detection. A WHO−approved laboratory has another 24 hours to confirm that the H5N1 bird flu virus has changed, either through mutation or through reassortment with human influenza. The strategy relies on WHO's global stockpile for rapid containment, three million treatment courses of Tamiflu. Quarantine, infection control measures and contact tracing must also be carried out.
WHO pandemic influenza draft protocol for rapid response and containment: http://www.who.int/csr/disease/avian_influenza/guidelines/pr otocolfinal30_05_06a.pdf
Source: http://news.yahoo.com/s/nm/20060530/hl_nm/birdflu_who_dc;_yl t=Aj5gqQjuQCW135X9kPdirroQ.3QA;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5 bmNhdA−−

31. *May 29, CNN* — **Six more bird flu cases in Indonesia.** Six more human cases of the H5N1 strain of avian flu have occurred in Indonesia, the World Health Organization has said. Three of the cases were fatal. That means 48 of the 224 human cases confirmed worldwide by the organization have occurred in Indonesia. Thirty−six of the Indonesian cases have proven fatal. Four of the infected people had been exposed to chickens or pigeon feces. Investigators are still looking into how the other two contracted the virus.
Source: http://edition.cnn.com/2006/HEALTH/conditions/05/29/birdflu. indonesia/

32. *May 28, Hindu (India)* — **Chikungunya disease sweeping through many Indian states.** Chikungunya, a viral disease transmitted by mosquitoes, is sweeping through Karnataka, Maharashtra and Andhra Pradesh, India. Thousands have been infected in the last three months. The disease has also spread to Tamil Nadu and Orissa. According to the World Health Organization, besides India, Chikungunya has been reported in the Indian Ocean islands of Mayotte, Mauritius and Seychelles since January 2006. In Karnataka, the number of people suspected to have been infected last month was 78,175.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://www.hindu.com/2006/05/28/stories/2006052802441100.htm

[Return to top]

Government Sector

33. *May 30, Edmonton Journal (Canada)* — **Courthouses to get airport−style security.** Courthouses in Sherwood Park and Fort Saskatchewan will be getting airport−style security systems as part of an $8.4 million security upgrade in four locations across Canada's Alberta Province. This follows similar security upgrades at the Edmonton Law Courts and the Calgary Court of Appeal. The security upgrades will include airport−style walk−through scanners, hand−held metal detectors, and X−ray inspection systems. More locations will be outfitted with

security equipment later this year. In total, these new measures will be in place in 75 locations throughout Alberta by the end of 2007. Perimeter security is part of the province's three−year comprehensive court security plan. Since similar measures were adopted in Edmonton and Calgary, sheriffs have prevented items such as pocket knives, box cutters, scissors, razor blades, screwdrivers, ammunition, drug pipes, and homemade brass knuckles from entering the courthouse, officials said
Source: http://www.canada.com/edmontonjournal/news/story.html?id=03ba1348−8de2−4b63−be28−83fc3d81e2da&k=60470

34. *May 30, Reuters* — **San Francisco City Hall evacuated over suspicious packages.** San Francisco City Hall was evacuated on Tuesday morning, May 30, after three suspicious packages were found in the building, officials said. "They have found several devices," a police duty official said. A bomb squad was at the scene investigating, as were police and sheriff's department officials. Several neighboring streets were closed off. San Francisco's early 20th century City Hall is one of the city's best known buildings.
Source: http://www.boston.com/news/nation/articles/2006/05/30/san_francisco_city_hall_evacuated_over_packages/

[Return to top]

Emergency Services Sector

35. *May 30, Government Accountability Office* — **GAO−06−518: Disaster Relief: Reimbursement to American Red Cross for Hurricanes Charley, Frances, Ivan, and Jeanne (Report).** In accordance with Public Law 108−324, the Government Accountability Office (GAO) is required to audit the reimbursement of up to $70 million of appropriated funds to the American Red Cross for disaster relief associated with 2004 hurricanes Charley, Frances, Ivan, and Jeanne. The audit was performed to determine if (1) the Federal Emergency Management Agency established criteria and defined allowable expenditures to ensure that reimbursement claims paid to the Red Cross met the purposes of the law, (2) reimbursement funds paid to the Red Cross did not duplicate funding by other federal sources, (3) reimbursed funds assisted only eligible states and territories for disaster relief, and (4) reimbursement claims were supported by adequate documentation. The 2004 hurricane season was one of the most destructive in U.S. history. Fifteen named storms resulted in 21 federal disaster declarations. Four hurricanes affecting 19 states and 2 U.S. territories from August 13 through September 26, 2004, triggered the nation’s biggest natural−disaster response up to that time. Over 150 deaths and $45 billion of estimated property damage are attributed to Hurricanes Charley, Frances, Ivan, and Jeanne in the United States alone. GAO is not making any recommendations in this report.
Highlights: http://www.gao.gov/highlights/d06518high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−518

36. *May 28, Pittsburgh Business Times* — **Emergency officials plan response to potential attacks at PNC Park.** As baseball fans in Pittsburgh, PA, watched the Pirates play the Cincinnati Reds Wednesday, May 17, they probably had no idea the air in and around PNC Park was being monitored for air−borne chemicals. Eight air−quality monitors lined various parts of the ballpark that night as part of preparations to make the stadium as safe as possible

when it hosts Major League Baseball's All−Star Game in July. The monitors alert officials to the presence of such chemical warfare agents as sarin and mustard gas. With the Midsummer Classic a mere six weeks away, tests and preparations for responding to possible emergencies −− not only at PNC Park, but across the city −− are becoming more frequent, local emergency planners say. PNC's location on the Allegheny River also adds another facet to efforts to defend it from a potential terrorist attack. In addition to in−stadium and air−borne threats, emergency responders also are working on "If by sea" defense scenarios.
Source: http://msnbc.msn.com/id/13029228/

37. *May 27, Arizona Daily Star* — **Rescuers training for electrical risks linked to hybrids.** The electricity flowing through the growing number of hybrid vehicles on the road poses a danger for rescue workers in crashes when one of these new vehicles gets into an accident. Hybrid cars and the large batteries within them could cause firefighters and rescue workers to be electrocuted when they are pulling passengers out of a car, said Tucson, AZ, fire department officials. The hybrid cars' electrical system consists of electrical lines that can be charged with a minimum of 144 volts and 100 amps −− enough to potentially kill any adult. Both the Tucson Fire Department and the Northwest Fire/Rescue District in 2004 underwent training to avoid a potentially fatal accident. In addition, firefighters are also undergoing training to deal with upcoming new safety features and hybrid models that will come out in 2007 or 2008.
Source: http://www.azstarnet.com/allheadlines/131040

38. *May 26, Government Accountability Office* — **GAO−06−645: Foreign Assistance: USAID Completed Many Caribbean Disaster Recovery Activities, but Several Challenges Hampered Efforts (Report).** In September 2004, Hurricane Ivan and Tropical Storm Jeanne passed through the Caribbean, taking lives and causing widespread damage in several countries. After initial U.S. emergency relief, in October 2004 Congress appropriated $100 million in supplemental funding, primarily for Grenada, Jamaica, and Haiti, which were significantly affected. The U.S. Agency for International Development (USAID), leader of the U.S. recovery programs, agreed, in consultation with the Office of Management and Budget, to complete the programs by December 31, 2005, giving the agency a 1−year time frame. The Government Accountability Office (GAO) was asked to (1) review the nature and status of the programs in Grenada, Jamaica, and Haiti as of December 31, 2005; (2) identify factors that affected the programs' progress; and (3) assess USAID's use of guidance and lessons learned from previous similar programs and efforts to draw lessons from the current programs. GAO recommends that the USAID Administrator (1) develop disaster recovery and reconstruction guidance that incorporates lessons learned from the current and previous programs and (2) revise staffing procedures to facilitate the rapid reassignment or hiring of needed personnel for postdisaster recovery and reconstruction programs. USAID agreed with GAO's recommendations.
Highlights: http://www.gao.gov/highlights/d06645high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−645

39. *May 25, Helicopter Association International (VA)* — **Five hour hurricane exercise puts helicopter fleet to the test.** State, federal, county and private−sector agencies conducted a full−scale exercise Thursday, May 25, designed to test their ability to jointly conduct a massive emergency rescue effort, in case a hurricane or other disaster strikes New Jersey. The exercise was coordinated by the State Exercise Support Team, which is part of the New Jersey Office of Homeland Security and Preparedness, headed by Director Richard L. Cañas. The exercise,

based at Atlantic City International Airport's Emergency Operations Center, involved nine helicopters deployed by the New Jersey Army National Guard, New Jersey State Police, U.S. Coast Guard, and the Eastern Region Helicopter Council. The helicopters flew from the Airport in Egg Harbor Township to three locations in Cape May Court House, Cape May County, to transport volunteers portraying emergency victims and rescue personnel. The five−hour exercise tested the ability of the various agencies to communicate with each other during a massive rescue operation. In particular, it tested the ability of helicopter pilots from so many diverse agencies to communicate via radio with each other and with ground control.
New Jersey Office of Emergency Management: http://www.ready.nj.gov/
Source: http://www.rotor.com/article.php?sid=3665&mode=thread&order= 0

[Return to top]

Information Technology and Telecommunications Sector

40. *May 30, VNUNet* — **Gartner: Firms must act now to fight Skype security threat.** Companies should "act now" to combat the growing security threat posed by Skype and other voice over IP telephony services, industry experts warned Tuesday, May 30. Analyst firm Gartner said that the latest vulnerability in the Skype for Windows client highlights the risk of using the application in enterprises. Lawrence Orans, a research director at Gartner, warned that, because the Skype client is a free download, most businesses have no idea how many Skype clients are installed on their systems nor how much Skype traffic passes through their networks. According to Gartner, businesses must assess the risks of using Skype for enterprise telephony and "take appropriate action."
Referenced Skype vulnerability: http://www.skype.com/security/skype−sb−2006−001.html
Source: http://www.vnunet.com/vnunet/news/2157124/firms−act−fight−sk ype−security

41. *May 29, Security Focus* — **Apache James SMTP denial−of−service vulnerability.** Apache James is prone to a remote denial−of−service vulnerability. Analysis: This issue is due to the application's failure to efficiently handle malformed SMTP commands. This issue allows remote attackers to consume excessive CPU resources of affected computers, potentially denying service to legitimate users.
Vulnerable: Apache Software Foundation James 2.2.
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/18138/references

42. *May 29, Associated Press* — **Survey: Middle class goes broadband as price falls.** Middle− and working−class Americans signed up for high−speed Internet access in record numbers in the past year, apparently lured by a price war among phone companies. Broadband adoption increased 59 percent from March last year to March 2006 among U.S. households with incomes between $30,000 and $50,000, according to a survey released Monday, May 29, by the Pew Internet and American Life Project. "It seems like the aggressive pricing strategies have had some effect for DSL providers in those middle−income segments," said John Horrigan, associate director for research at Pew. The average monthly fee for DSL was $32 in December, compared to $41 for cable. A year and a half earlier, DSL cost almost as much as cable.
Survey: http://www.pewinternet.org/pdfs/PIP_Broadband_trends2006.pdf
Source: http://news.yahoo.com/s/ap/20060529/ap_on_hi_te/broadband_ac

cess;_ylt=Ard2RFMN.RIRjPvPu_IERDwjtBAF;_ylu=X3oDMTA5aHJvMDdw BHNlYwN5bmNhdA−−

43. *May 27, eWeek* — **Symantec Plugs Anti−Virus worm hole in record time.** Working feverishly through the holiday weekend, Symantec's security response team has completed patches for a "high−risk" worm hole in two enterprise−facing product lines. The flaw, which could allow malicious hackers to take complete control of a system without any user action, was discovered and reported by eEye Digital Security. In an advisory posted Saturday, May 27, Symantec described the issue as a stack overflow affecting the Symantec Client Security and Symantec Anti−Virus Corporate Edition. The company's advisory is a confirmation of eEye's earlier warning that the flaw could lead to a self−propagating worm without any user action. Symantec's advisory: http://www.symantec.com/avcenter/security/Content/2006.05.25 .html Source: http://www.eweek.com/article2/0,1895,1968603,00.asp

44. *May 26, VNUNet* — **Gartner: Open source software storms database charts.** Open source databases are showing the highest growth rate in the database market, according to a new study by analyst firm Gartner. "The combined category of open source database management systems [DBMS] vendors, which includes MySQL and Ingres, showed the strongest growth, although it was one of the smallest revenue bases, " said Colleen Graham, a principal analyst at Gartner. "These open source DBMS products continue to improve in functionality and scalability, and DBMS tool vendors are beginning to provide support for these offerings," stated Graham. Source: http://www.vnunet.com/vnunet/news/2156990/open−source−storms −database

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 continues to receive reports of data theft that targets online users and Federal government web sites. Recently, Veteran Affairs data was stolen from the home computer system of a Veterans Affairs (VA) employee. This data contained large amounts of personally identifiable information, such as, names, social security numbers, and dates of birth. Over 26 million veterans and some spouses are affected by this incident. The VA is continuing to investigate this issue and working to inform affected parties of this incident so that the appropriate steps can be taken to protect against this information being misused. US−CERT recommends that users take the following measures to protect against data theft:

Encrypt sensitive data on your local hard drive and back up mediums.

Attend Security Awareness training to gain a better understanding of your organization's policies and procedures for handling sensitive data.

Restrict access to sensitive data from Internet connected systems.

For additional information, please review the following URL:
http://www.first.gov/veteransinfo

Active Exploitation of a Vulnerability in Microsoft Word

US−CERT is currently researching a zero day vulnerability in Microsoft Word. US−CERT and Microsoft will continue to investigate the public reports to help provide additional guidance as necessary. There is currently no patch available for this vulnerability. For more information please review the following:

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

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

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

PHISHING SCAMS

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

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

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

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 38566 (−−−), 445 (microsoft−ds), 50497 (−−−), 80 (www), 135 (epmap), 25 (smtp), 113 (auth), 53 (domain) 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