Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 08 July 2005

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

Daily Highlights

- The Transportation Security Administration has made changes to the security checkpoint at Pennsylvania's Pittsburgh International Airport in response to an incident last week in which a woman skirted the metal detectors and boarded a plane to Houston. (See item 8)
- In light of Thursday's attacks in London, the United States Government raised the threat level from Code Yellow – or Elevated – to Code Orange – or High – targeted only to the mass transit portion of the transportation sector. (See item 9)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

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://esisac.com]

1. *July 07, Washington Post* — **Imported gas cited in rash of leaks.** Washington Gas utility officials said on Wednesday, July 6, that a change from domestic to imported natural gas was the "key contributing factor" in a rash of leaks in underground mains and service lines in Prince George's County, MD, over the past two winters. A company−sponsored study, launched after a house exploded in late March, found that subtle molecular differences in the imported liquefied natural gas the utility began using in August 2003 were drying the rubber seals of aging metal couplings that link sections of pipe. The frequency of leaks began to soar in late 2003, soon after the company started supplying Prince George's with imported gas, mainly from Trinidad, brought in by tanker through Cove Point liquefied natural gas terminal in Calvert County, MD.

Cove Point officials sharply disagreed with the Washington Gas interpretation of the study. An analysis performed by Dominion Resources Inc., which operates the terminal, found that the chemical makeup of gas from its facility closely matched gas generally used in the Washington Gas system. The findings are certain to intensify discussion in the gas industry about "interchangeability" −− the feeding of different natural gases, including imported liquid natural gas, into the U.S. interstate pipeline grid.
Report and fact sheet: http://www.washingtongas.com/library/general/media_kit.cfm
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/06/AR2005070602284.html

2. *July 07, The Arizona Republic* — **Nuclear reactor shut down again.** One week after returning from a five−week shutdown, one of three reactors at Palo Verde nuclear power plant again closed due to a leaking oil seal. Plant operator APS said it's the same problem that prompted the May 22 closing of Unit 3 at Palo Verde Nuclear Generating Station, located about 50 miles west of Phoenix, AZ. The utility discovered that one of two new reactor coolant pump oil seals was not working properly, so plant managers shut down the reactor shortly after midnight Wednesday, July 6, to fix the problem and attempt to figure out why it recurred, said APS spokesperson Jim McDonald. The utility expects it will take one week to repair the leaking coolant pump, which is used to pump water from the reactor to the steam generator to help produce electricity. Despite closing the nearly 1,300−megawatt reactor during summer heat, utility officials said there should be plenty of power available for the Phoenix area over the next week.
Source: http://www.azcentral.com/business/articles/0707paloverde07.h tml

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *July 07, Washington Post* — **Boeing may be fined for exported technology.** Boeing Co. is in talks with the Department of State about alleged violations of arms control laws related to the sale of 96 civilian aircraft and spare parts to China from 2000 to 2003, company and Department of State officials said on Wednesday, July 6. The company said the talks concern the sales of planes that contain a gyrochip that helps with stability of the aircraft but can also be applied to missiles. Kurtis Cooper, a Department of State spokesperson, confirmed the inquiry, saying the department is in negotiations with Boeing "regarding potential violations" of the export laws, and, "If and when these negotiations result in a settlement, the documents related to the charges, including the terms of that settlement, will be made public." The aerospace industry has complained for years that export control regulations are cumbersome and ill−suited for the current marketplace, where commercial and defense technology is increasingly interchangeable. The rules often delay deals and put U.S. firms at a competitive disadvantage in foreign competitions, company officials have argued.

Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/06/AR2005070602262.html

[Return to top]

Banking and Finance Sector

4. *July 07, Financial Times (UK)* — **UK companies reach for disaster recovery plans.** Companies in central London scrambled to implement disaster recovery plans and make arrangements for customers and staff amid the fallout from the terror attacks on Thursday, July 7. Several banks closed London branches, however, the biggest problem for all companies remained how to get staff home. Barclays bank said it used a river service from its Canary Wharf headquarters and had also hired a number of buses to get staff to outer London train services. The Association for Payment Clearing Services, the United Kingdom payment association, said banking services operated normally. Stella Littlewood, human resources director at Arup, the engineering group, said, “We have a disaster recovery plan and as soon as we heard about the blasts, everyone jumped into action. We’ve put everything in place for a worst−case scenario in the hope that we won’t have to use it. We’ve doubled our security, done an audit of each of our offices, and we’ve compiled a list of those that are unaccounted for. One of the difficulties in establishing contact is that the mobile networks are proving difficult to use.” Dan Bridgett of the London Chamber of Commerce said, “This is an unpleasant wake up call for companies without continuity plans.”
   Source: http://news.ft.com/cms/s/ce325258−eef3−11d9−8b10−00000e2511c 8.html

5. *June 22, Harbor Light (MI)* — **Michigan State police announce identity theft team.** The Michigan State Police (MSP) Region I Special Investigation Division is now better prepared to combat the fastest growing crime in the nation with the creation of a full−time Identity Theft Team. "The creation of this Identity Theft Team is an example of the Michigan State Police effectively responding to emerging crime trends with new techniques and new solutions," said Detective First Lieutenant David Peltomaa, commander of the Special Investigation Section, which oversees the Identity Theft Team. The Identity Theft Team investigates cases involving the theft or misuse of personal identification information to obtain goods, services, credit and fraudulent bank accounts or to facilitate other criminal activity. The most common type of personal identification information misused is the numbers from Social Security cards, driver’s licenses, credit and debit cards and bank accounts. The Team’s primary focus is assisting law enforcement officers and agencies with large scale investigations, as well as investigating cases with out of state victims where the suspect resides in Michigan.
   MSP Identity Theft Team: http://www.michigan.gov/identity−theft
   Source: http://www.harborlightnews.com/News/2005/0622/Local_News/028 .html

[Return to top]

Transportation and Border Security Sector

6. *July 08, The Christian Science Monitor* — **U.S. vigilant on rail systems after UK bombing.** From Boston to Chicago to Los Angeles, security was stepped up in mass transit systems on

Thursday, July 7. In New York's Grand Central Terminal, commuters were greeted with the sight of blue−clad police officers armed with automatic weapons on Thursday. The police were also much more noticeable in the subway system. "We're definitely increasing police presence. We've tightened security measures," says Lydia Rivera, of the Massachusetts Bay Transportation Authority in Boston. "But overall, we are just going to run business as usual." In Chicago, police increased their presence in train stations and brought in bomb−sniffing dogs. Frank Kruesi, president of the Chicago Transit Authority, said, "We have people trained to pay attention −− employees and increasingly customers." Since 9/11, security has been tightened on Amtrak and in subways in the form of increased police presence, random searches by bomb−sniffing dogs, and significantly boosted security training for personnel. In most major train stations, trash cans are now bomb−resistant, and agents specially trained in biohazards and explosives routinely patrol. The Department of Homeland Security has also allocated $115 million to help urban areas increase security of mass transit. And immediately after the Madrid bombings, it hired 100 new rail security inspectors.
A list of security measures being taken around the country is available from CNN:
http://www.cnn.com/2005/US/07/07/cities.security/index.html
Amtrak statement on raising the security threat level:
http://www.amtrak.com/servlet/ContentServer?pagename=Amtrak/ HomePage
Source: http://www.csmonitor.com/2005/0708/p01s02−usgn.html

7. *July 07, Associated Press* — **Public transit systems hard to protect.** Subway systems are inviting targets for terrorists because they are difficult to secure. The kind of screening equipment used to check passengers at airports can't be used because it's too slow for systems designed to quickly move large numbers of people. "Mass transportation systems will always be vulnerable to some extent if we want to keep them as efficient as they are today," said Rafi Ron, president of the Washington−based transportation security consulting firm, New Age Solutions. About 29 million people take commuter trains, subways and buses daily in the U.S., with the New York City area accounting for about a third of the total, said Alan Pisarski, a Washington−based national transportation policy analyst. The next−largest systems are Chicago, Washington, Boston, and Philadelphia. James Carafano, a homeland security expert with the Heritage Foundation think tank, said trains are a tempting target for terrorists because they're so predictable.
Source: http://www.nytimes.com/aponline/national/AP−Vulnerable−Train s.html?oref=login

8. *July 07, Pittsburgh Post−Gazette (PA)* — **Chains go up to prevent airport security lapses.** The Transportation Security Administration (TSA) has made changes to the security checkpoint at Pennsylvania's Pittsburgh International Airport in response to an incident last week in which a woman skirted the metal detectors and boarded a plane to Houston, TX. TSA officials have installed chains between the checkpoint's detectors and X−ray machines to prevent people from slipping between the two pieces of equipment. The changes were made after an unidentified woman placed her carry−on bags on the X−ray machine and then squeezed through an open space, not more than a foot wide, between the machine and the walk−through metal detectors June 29. The TSA has said the woman did so unintentionally. Lauren Stover, a TSA spokeswoman, said the agency eventually plans to install Plexiglas between the metal detectors and the X−ray machines to "permanently resolve any open areas" that potentially could be used to slip past security. The TSA is also conducting an investigation to determine exactly how the woman was able to slip past screeners without going through the metal detectors and whether

anyone should be disciplined as a result of the incident.
Source: http://www.post−gazette.com/pg/05188/534086.stm

9. *July 07, Department of Homeland Security* — **Threat level change targeted to mass transit sector.** Department of Homeland Security (DHS) Secretary Michael Chertoff announced a targeted raise in the threat level on Thursday, July 7. "In light of Thursday's attacks in London, the United States Government is raising the threat level from Code Yellow – or Elevated – to Code Orange – or High – targeted only to the mass transit portion of the transportation sector. This only includes regional and inter−city passenger rail, subways and metropolitan bus systems. DHS is also asking for increased vigilance in other transportation systems. DHS has stood up the Interagency Incident Management Group to ensure full situational awareness around this incident and in the United States. DHS does not have any specific intelligence indicating this type of attack is planned in the United States. However, the tactics and methods of terrorists are known, as demonstrated by the horrific rail bombings in Madrid last year. The intent of al Qaeda and affiliated organizations to attack in Europe and the United States has been well documented and continues to be reflected in intelligence reporting."
Transcript from Secretary Chertoff's press briefing:
http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0700.xml
Secretary Chertoff's official statement on the bombings:
http://www.dhs.gov/dhspublic/display?content=4577
Source: http://www.dhs.gov/dhspublic/index.jsp

[Return to top]

Postal and Shipping Sector

10. *July 07, Reuters* — **UPS to open hub in China.** UPS Inc., the world's top package carrier, signed an agreement on Thursday, July 7, to set up a logistics distribution center in China. Ken Torok, Asia−Pacific head for UPS, said the Atlanta, GA, based firm also planned to expand its fledgling domestic express service next year, pitting it against national monopoly China State Postal Bureau (China Post). UPS's hub, designed to have an annual capacity of 200,000 tons, will be based at Shanghai's international airport and is expected to begin operations in January 2007. UPS joins rivals including Dutch logistics firm TPG and Deutsche Post's DHL Express rushing to widen their footprint in a $1.5 billion market that industry executives expect to become the world's largest cargo market some day. Transport hubs −− such as the one UPS is envisioning in China's commercial stronghold Shanghai −− act as distribution centers by taking packages and shipping them on to their final destinations. Torok said UPS' hub agreement was the first among foreign carriers.
Source: http://today.reuters.com/investing/financeArticle.aspx?type= mergersNews&storyID=2005−07−07T073810Z_01_SHA45196_RTRIDST_0 _TRANSPORT−CHINA−UPS.XML

11. *July 06, Baseline Magazine* — **Postal Service to institute barcode mail tracking.** If the U.S. Postal Service (USPS) has its way, "the check is in the mail" excuse will no longer be valid. The company that sent you the bill could verify whether you're bluffing through a bar code on the return envelope scanned by the USPS. That tracking system, which starts this month, is one way the Postal Service is making first−class mail such as bills and personal correspondence

more valuable. USPS says a financial institution will test the system in July by using the new bar code. The customer will track mail as it winds through the Postal Service's 283 processing and distribution centers across the country. Currently, mail is mostly scanned at the beginning and delivery points. By year's end, all letter mail could be tracked at Postal Service facilities. The Postal Service will add commercial customers throughout 2006.
Source: http://www.baselinemag.com/article2/0,1397,1834515,00.asp

[Return to top]

Agriculture Sector

12. *July 07, Courier−Journal (KY)* — **Strangles suspected in horse at Ellis Park.** The Kentucky veterinarian's office said Wednesday, July 6, a horse stabled at Churchill Downs owned Ellis Park in Henderson, KY, was removed from the racetrack Saturday, July 2, after coming down with a suspected case of the strangles bacterial disease. Rusty Ford, equine programs manager for the veterinarian's office, said he's optimistic that the horse was taken from Ellis before becoming contagious. The horse's barn has been placed under a state quarantine. The strangles bacteria typically causes fever, breathing difficulties, and swelling of the lymph nodes.
Source: http://www.courier−journal.com/apps/pbcs.dll/article?AID=/20050707/BUSINESS/507070351/1003

13. *July 06, Associated Press* — **Anthrax found in two North Dakota cattle herds.** Authorities in North Dakota have quarantined two cattle herds after detecting anthrax. Veterinarians said the discovery was expected, because recent heavy rains were likely to stir up dormant anthrax spores. Beth Carlson, a deputy state veterinarian, said Wednesday, July 6, the herds were located in the Sheyenne River valley in Ransom County, in southeastern North Dakota. The suspected cases were confirmed at a North Dakota State University veterinary lab, Carlson said. Anthrax spores are frequently present in the soil, and can become active in moist conditions. They can be inhaled or ingested by livestock.
Source: http://www.grandforks.com/mld/grandforks/12068839.htm

14. *July 06, DTN News* — **More soybean rust found in Florida.** Florida agriculture officials have confirmed another case of Asian soybean rust, this time on a kudzu plant in Gadsden County in the state's panhandle. The soybean rust detection was determined following a Polymerase Chain Reaction (PCR) test, used to confirm the presence of the disease. Jim Walker, a Florida Department of Agriculture pest survey specialist, told DTN the location of the rust−infected kudzu plant was three miles from a University of Florida research facility in Quincy, FL. Gadsden County is just south of Seminole County, GA, where rust has already been detected in 2005. "The intensity of infection on the plant was thought to be light," Walker said. "However, this is in an area where most of Florida's soybean production is located."
Source: http://www.dtnsoybeanrustcenter.com/index.cfm?show=10&mid=61 &pid=18

15. *July 06, Associated Press* — **Anthrax found on two West Texas ranches.** Two Sutton, TX, ranches are under quarantine after the discovery of anthrax in several head of cattle, horses, and deer, state authorities said Wednesday, July 6. Pascual Hernandez, an agent with the Texas Cooperative Extension Service in Sonora, said several other ranches have reported livestock

and deer deaths and are being investigated. The ranches where the anthrax has been found will be under quarantine until veterinarians can determine that no other animals are infected, a process that could take six months to complete. The disease associated with grazing animals is not normally transmitted to humans, except by eating tainted meat or through exposure, via open wounds, to infected material. In rare situations, anthrax can become airborne and be inhaled. Thurman Fancher, West Texas area director and veterinarian for the Texas Animal Health Commission, said it is important to notify the public of an outbreak. He said livestock on infected property must be vaccinated and neighboring ranchers also must be notified of the need to vaccinate their herds.
Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/325574 5

16. *July 06, Maui News (HI)* — **State of Hawai`i tightens laws on theft from farms, ranches.** On Friday, July 1, Hawai`i Governor Linda Lingle signed into law two bills designed to make it easier to battle agricultural theft and trespassing on farmlands. Theft from farms and ranches is a multimillion−dollar problem in the islands. Act 181 establishes the offense of criminal trespass in the second degree if a person enters or remains on agricultural lands without permission. Act 182 lowers the amount of farm produce covered by the ownership and transportation certificate to 25 pounds, and making possession of that amount of farm commodities or products without a certificate prima facie evidence that the items are or once were stolen. Act 182 also makes it a felony to steal agriculture equipment, supplies, or products valued between $100 and $20,000, or agricultural products that exceed 25 pounds. Possession of aquacultural products or livestock without proper ownership or movement certificates is similarly covered. Jason Moniz, the livestock disease control program manager at the state Department of Agriculture, said that until now, even if a farmer saw someone driving out his gate with a truckload of stolen animals or produce, the police “could only stop him for speeding. They couldn’t stop them for the purpose of checking” the origin of the property.
Source: http://www.mauinews.com/story.aspx?id=10307

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

17. *July 06, Environmental Protection Agency* — **EPA reminds utilities of looming arsenic deadline.** The U.S. Environmental Protection Agency (EPA) is reminding water systems that a new, more protective national standard for arsenic in drinking water will take effect less than six months from now. The EPA adopted the new standard in 2001 that requires all drinking water systems to reduce arsenic from the current standard of 50 parts per billion to 10 parts per billion. The main areas affected in the western U.S. include small water utilities that draw their drinking water from deep underground wells in California’s foothills and Central Valley, and throughout Arizona and Nevada. The EPA estimates that nationwide, roughly 97 percent of the utilities that fail to meet the new standard are the smaller systems, which serve fewer than

10,000 people. The EPA estimates that the new standard will provide greater protection from cancer risks and other health problems. Ingesting too much arsenic can lead to lung, bladder, liver, skin and other cancers, as well as damage to the cardiovascular, pulmonary, immune, neurological, and endocrine systems. The EPA, state and local agencies are providing information and technical assistance to utilities that have yet to install treatment systems or take alternative approaches to reduce arsenic levels.
Source: http://yosemite.epa.gov/r9/r9press.nsf/7f3f954af9cce39b882563fd0063a09c/8b1158dd81329dc188257036006882ff!OpenDocument

[Return to top]

Public Health Sector

18. *July 07, Associated Press* — **Update: Bird flu not behind death in Cambodia's influenza outbreak.** The death of a 20−year−old Cambodian man, Meas Met, was due to an outbreak of human influenza−not bird flu as some had feared, a World Health Organization (WHO) official said Thursday, July 7. Test results showed Met had the H3N2 type of the influenza A virus−not the H5N1 bird flu strain that has devastated poultry stocks and killed at least 54 people in Southeast Asia, WHO epidemiologist Megge Miller said. The H3N2 virus commonly circulates among humans, according to Miller. The victim, from an orphanage in the capital, Phnom Penh, died Tuesday, July 5. Influenza type A or B cause epidemics almost every year around the world, according to the US Centers for Disease Control and Prevention (CDC), which estimates that an average of about 36,000 Americans die from flu complications each year.
Source: http://asia.news.yahoo.com/050707/ap/d8b6emg84.html

19. *July 07, Independent (NJ)* — **Board of Health forms Medical Reserve Corps.** In order to provide additional protections for residents, the Monmouth County, NJ Board of Health is establishing a Medical Reserve Corps unit to strengthen the public health infrastructure and improve response capabilities in the event of an emergency. The Medical Reserve Corps (MRC) program was launched officially as a national community−based movement in July 2002. It was formed in response to President Bush's call for Americans to offer volunteer service in their communities. The World Trade Center disaster on September 11, 2001, and the anthrax reports that followed reinforced the need for pre−identified and trained supplemental medical and public health personnel to assist with emergency operations such as mass antibiotic dispensing or mass immunization campaigns. The MRC is a charter program of the Citizen Corps. The Monmouth County Health Department has a pool of some 200 citizens−both medical and nonmedical−who stand ready to react and serve the Health Department in the event of emergencies of unforeseen incidents that require a public health response. Members are required to complete basic training and participate in exercises and drills throughout the year. Medical Reserve Corps units already exist in New Jersey's Bergen, Essex, Hudson, Hunterdon, Middlesex, Morris, Somerset, Sussex and Union counties.
Source: http://independent.gmnews.com/news/2005/0707/Front_Page/035. html

20. *July 07, Xinhua News (China)* — **SARS vaccine trial runs smoothly to second stage.** A total of 300 volunteers will take part in the second−phase human trials of a SARS (severe acute respiratory syndrome) vaccine. Zhong Nanshan, president of Chinese Medical Association, stated scientists in Beijing will carry out trials among volunteers aged 20 to 60 to test the

effectiveness of the vaccine in human beings. According to Yin Hongzhang−an official from China's State Drug Administration, which is in charge of supervising trials of any new vaccine or drug−the first phase trials involved 36 volunteers at the Sino−Japanese Friendship Hospital in Beijing on May 22, 2004. By early December 2004, antibodies against the disease were found in all volunteers, without obvious side effects. The vaccine was produced by Beijing's Sinovac Biotech Company Ltd in 2004 after SARS emerged in 2003 and again in 2004, leaving at least 350 dead, mostly in China. The 300 volunteers in the second trial will undergo various medical examinations to record the persistence of antibodies over a nine−month period after the vaccine is administered, according to Nanshan. Experts say only after a vaccine has passed three phases of human trials will it be licensed for use on the public.
Source: http://news.xinhuanet.com/english/2005−07/07/content_3187227 .htm

21. *July 07, Agence France Presse* — **Indonesian polio cases climb to 122.** The World Health Organization (WHO) said the number of children affected by the crippling polio virus in an outbreak in Indonesia has risen to 122 with the confirmation of 11 new cases. Spokesperson Sari Setiogi said there were no immediate details on the location or circumstances of the latest infections, which come amid a major immunization program to halt the spread of the disease. Some 6.5 million children have been vaccinated since the first case of polio in almost a decade in Indonesia was detected in April. Authorities hope to target 24 million more children in a two−month campaign beginning in August. Polio is believed to have returned to Indonesia via Saudi Arabia, either through migrant workers or Islamic pilgrims returning from Mecca, who may have passed on a strain of the virus originating in Nigeria.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050707/hl_afp /healthindonesiapolio_050707110735

22. *July 07, Associated Press* — **Malaysia tightens medical screening for foreign workers.** Malaysia has tightened its medical screening of foreign workers to control the spread of contagious diseases including AIDS, Health Minister Chua Soi said Thursday, July 7. Beginning next month, foreign workers must be tested within a month of their arrival for HIV, hepatitis B, syphilis, tuberculosis, leprosy and other diseases, Soi told reporters. Under current regulations, workers are required to provide medical certificates from their home countries to prove they are healthy before being allowed to enter Malaysia. They must undergo medical screening in Malaysia after one year when applying for an extension of their work permits. Soi said the new ruling would be effective in eliminating unhealthy workers; those found with communicable diseases will be deported. Malaysia is heavily reliant on foreign workers and the new medical rule is part of reforms being carried out by the government in its treatment of guest labor.
Source: http://asia.news.yahoo.com/050707/ap/d8b6g1fo0.html

23. *July 06, University of California, Los Angeles* — **UCLA scientists reveal how Nipah virus infects cells; discovery could counteract use of deadly virus for bioterrorism.** UCLA scientists have discovered how the deadly Nipah virus infiltrates human cells to cause encephalitis, or brain inflammation. Designated as a potential bioterrorism agent by the National Biodefense Research Agenda, the virus exploits a protein essential to embryonic development to enter cells and launch its attack. "In its natural state, the Nipah virus can be used as a potential bioterrorism agent capable of devastating an entire country's public health and economy," said Dr. Benhur Lee, principal investigator and UCLA assistant professor of

microbiology, immunology and molecular genetics. Since 1998, the Nipah virus has triggered disease outbreaks in Australia, Singapore, Malaysia and Bangladesh. Animals spread the virus to people, where it causes life−threatening respiratory and neurological diseases that kill up to 70 percent of patients — a danger level equivalent to the Ebola virus. To infect a cell, viruses must bind to a viral−specific receptor on the cell's surface in order to penetrate it. Lee's team identified a cell receptor called Ephrin−B2 as the key used by the Nipah virus to unlock the cells. Ephrin−B2 is found in humans, horses, pigs and bats, which may explain why the infection can jump so easily from one species to another.
Source: http://newsroom.ucla.edu/page.asp?RelNum=6292

24. *July 06, Reuters* — **UnitedHealth to buy PacifiCare.** UnitedHealth Group Inc. (UNH.N), the second largest U.S. health insurer, on Wednesday, July 6, said it agreed to buy PacifiCare Health Systems Inc. for about $8.1 billion in cash and stock, in a deal that would expand its services for senior citizens. Under the terms of the agreement, UnitedHealth said it would pay 1.10 shares of its stock, plus $21.50 in cash, for each share of PacifiCare. The merger would make the combined company a stronger challenger to industry−leader WellPoint Inc. (WLP.N), which has more than 28 million subscribers after its acquisition of Anthem Inc. last year. PacifiCare, with about 3 million members, is one of the biggest private providers of health plans to Medicare, a US government program that provides the elderly and some disabled people with health insurance. UnitedHealth has about 23.2 million members. The deal could face anti−trust scrutiny because of the combined company's potential market power in States such as California and Texas, according to one health care investment banker who was not involved in the deal. The deal marks the latest push toward consolidation by US health insurers trying to gain more leverage to bargain for cheaper rates from hospitals and drug makers.
Source: http://www.nytimes.com/reuters/business/business−health−paci ficare.html?

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

25. *July 08, The Guardian (UK)* — **Emergency plan and call surge hit phones.** Londoners found themselves unable to contact friends and family in the aftermath of the attacks on Thursday, July 7, as government action and widespread panic combined to disrupt the capital's telephone network. A surge in calls after the explosions put the communications system under extreme pressure, with BT saying the sheer volume of calls was causing delays. But some of the downtime was the result of a government emergency plan known as Access Overload Control coming into effect. This allows various parts of the telephone network to be shut down completely or prioritized for use by the emergency services. Parts of London came under these restrictions during the course of Thursday.
Source: http://www.guardian.co.uk/uk_news/story/0,3604,1523609,00.ht ml

26. *July 07, Computerworld* — **Tsunami warning hits the spam barrier.** The first live run of the Indian Ocean tsunami warning system earlier this month produced an unexpected result for some users of Apache's SpamAssassin. Subscribers to the automated e−mail warning system, which sent out an alert for an earthquake off Northern Sumatra that rated 6.7 on the Richter scale, found that the tsunami warning notification deferred as spam. The problem arises if the open−source filter is installed straight out of the box; the messages, usually written in uppercase, are not considered spam. But for anyone who locks down the spam filter, SpamAssassin categorizes the e−mail as spam due to a combination of uppercase text in a clear−cut format forwarded by a hidden sender. With the spam filters locked down, the warning message−−written in the original in uppercase letters as "THERE IS A VERY SMALL POSSIBILITY OF A DESTRUCTIVE LOCAL TSUNAMI IN THE INDIAN OCEAN"−−rates a spam score of 3.7 out of 10.
Source: http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,102996,00.html

27. *July 06, The Courier Times (NC)* — **College teams with town on public safety center.** Piedmont Community College (PCC) and the town of Yanceyville, NC, are taking an empty textile mill and turning it into a center that will train law enforcement officers and bring much−needed economic development to Caswell County. Through the effort, the Yanceyville Municipal Annex, which once served as a textile mill, will house the Yanceyville police department, public works, and PCC's Public Safety Training Center. The partnership between college and municipality also includes teaming up with Dan River Prison Work Farm. According to Dan River Superintendent George Solomon, inmates at Dan River will provide much of the labor to renovate the old cotton mill, explained Solomon. Dr. H. James Owen, PCC president, said the Public Safety Training Center would allow the college to provide additional professional development programs. The college expects more than 1,000 individuals each year to receive training at the Public Safety Training Center.
Source: http://www.thestate.com/mld/thestate/news/local/12068208.htm

28. *July 06, Associated Press* — **South Carolina's statewide safety radio network up and running.** A statewide radio network that lets police, fire and other emergency workers in South Carolina talk to each other has passed a couple of major real−world tests and is ready for hurricane season. Without it, people who needed to respond to disasters were like cell−phone subscribers without roaming privileges and "No Service" appeared on their screens. In all, 200 different law enforcement and emergency agencies were able to easily communicate on the system, said George Crouch, who runs the program for the state Budget and Control Board. The state also brought in a mobile tower to handle the extra traffic, Crouch said. And it has a transmitter that can be carried aloft by a plane or helicopter to handle needs, Crouch said. So far, nearly 18,000 of the new radios are in the hands of police and other emergency workers statewide, making South Carolina's system the most interoperable in the nation, Crouch said.
Source: http://www.wsoctv.com/news/4690549/detail.html

[Return to top]

Information Technology and Telecommunications Sector

29.

July 07, vnunet.com (UK) — **Suspected spammer Smith seized.** Suspected spammer Christopher Smith, nicknamed the Rizler was arrested at a Minneapolis, MN airport shortly after stepping off a flight from the Dominican Republic, where he had been operating since a U.S. federal judge in May shut down his companies, Burnsville Internet and Xpress Pharmacy Direct, and ordered him to stop selling drugs online. Smith had since set up similar operations in the Dominican Republic, through which he is alleged to have sent more than a billion spam emails either to AOL email addresses or through AOL email accounts. The FBI claims that Smith has already made about $18 million this year. Federal authorities raided Xpress Pharmacy and Smith's home on 10 May, seizing his passport and $4.2m in assets, including a $1.1m house and luxury cars worth $1.8m. At the same time the FBI closed down his 85−employee company. Investigators concluded that Smith had been selling medicines to customers without proper prescriptions, and selling drugs without a licence. The U.S. Attorney's office claims that Smith had broken court orders and is recommending that he be held in criminal contempt and jailed for six months.
Source: http://www.vnunet.com/vnunet/news/2139427/spam−supremo−smith −sued

30. *July 06, FrSIRT* — **PHPWebSite SQL Injection and Cross site scripting vulnerabilities.** Multiple vulnerabilities were identified in PHPWebSite, which could be exploited by malicious users to conduct SQL injection, cross site scripting and directory traversal attacks. These flaws are due to an input validation error in the search module that does not properly filter a specially crafted "mod" parameter, which could be exploited by remote attackers to conduct SQL injection, cross site scripting and directory traversal attacks. PHPWebSite version 0.10.1 and prior are affected.
Users should apply the patch: http://phpwebsite.appstate.edu/downloads/security/phpwebsite_security_patch_20050705.2.tgz
Source: http://www.frsirt.com/english/advisories/2005/0993

31. *July 06, Security Focus* — **McAfee IntruShield Security Management System multiple vulnerabilities.** McAfee IntruShield Security Management System is susceptible to multiple vulnerabilities. The first two issues are cross−site scripting vulnerabilities in the 'intruvert/jsp/systemHealth/SystemEvent.jsp' script. These issues are due to a failure of the application to properly sanitize user−supplied data prior to utilizing it in dynamically generated HTML. The next two issues are authorization bypass vulnerabilities leading to information disclosure and the ability to acknowledge, de−acknowledge, and delete security alerts. These vulnerabilities require a valid user account in the affected application. Users of affected packages should contact the vendor for further information on obtaining fixes.
Source: http://www.securityfocus.com/bid/14167/exploit

32. *July 06, FrSIRT* — **IBM Lotus Notes HTML attachments script execution vulnerability.** A vulnerability was identified in IBM Lotus Notes email client, which could be exploited to conduct cross site scripting attacks. The problem is that JavaScript code included in HTML attachments is not properly sanitised before being displayed, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. IBM Lotus Notes 6.5.4 and prior are affected. No official patch is known at this time.
Source: http://www.frsirt.com/english/advisories/2005/0995

33.

July 06, The Register (UK) — **Micrsoft UK defaced in hacking attack.** Microsoft's UK Website was defaced by well−known defacer Apocalypse Tuesday, July 5, with a message in support of Venezuelan hacker Rafa. The site has since been restored to normal operation and the offending GIF removed. A Microsoft spokesman said it was aware of the attack, which technical staff are investigating. "There is no reason to believe customer data or any other sensitive information has been compromised," he said. Apocalypse has been targeting U.S. institutions and the government sites for months, always posting messages in support of Rafa Nunez−Aponte, a suspected member of the World of Hell hacking crew. Rafa is in custody in the U.S. following his arrest in Miami, FL, in April over a series of alleged attacks on U.S. Department of Defense servers dating back to 2001. Previous targets of Apocalypse's "digital graffiti" attacks have included Stanford University and U.S. Navy Websites.
Source: http://www.theregister.co.uk/2005/07/06/msuk_hacked/

34. *July 05, Adobe* — **Buffer overflow vulnerability in Adobe Reader.** A vulnerability within Adobe Reader has been identified within the Adobe Reader control. If exploited, it could allow the execution of arbitrary code under the privileges of the local user. Remote exploitation is possible if the malicious PDF document is sent as an email attachment or if the PDF document is accessed via a web link.
Linux or Solaris users: download Adobe Reader 7.0 at
http://www.adobe.com/products/acrobat/readstep2.html.
IBM−AIX or HP−UX: download Adobe Reader 5.0.11 at
http://www.adobe.com/products/acrobat/readstep2.html.
Source: http://www.adobe.com/support/techdocs/329083.html

35. *July 04, EE Times* — **U.S. Air Force taps secure ultrawideband.** Sandia National Laboratories has combined ultrawideband (UWB) radio signals with advanced encryption techniques to develop a secure sensor and communications network for the U.S. military. The ultrasecure UWB communication system promises to help the government protect its troops on the battlefield by detecting the position of enemies and by making it much harder for them eavesdrop or jam military communications. "By utilizing the immense spectrum of UWB to spread the energy of communications signals from sensors over a wide frequency spectrum, the signal power falls below the noise floor of normal receivers," said Sandia National Laboratories researcher Timothy Cooley. Also known as "impulse radio," ultrawideband radio transmissions smear a wide spectrum with short, 100−picosecond pulses that are below the noise floor of conventional radio receivers. Even if enemies were equipped with a special UWB receiver, they would be unlikely to know how to reassemble the disparate data packets of each impulse into a coherent whole. And even if they should manage to reassemble the packets, they would still have to crack the 256−bit AES encryption used by Sandia's special secure military communications version. The sensor and communications networks are being developed for the U.S. Air Force Electronic Systems Center.
Source: http://www.eetimes.com/news/latest/technology/showArticle.jhtml?articleID=165600118

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 reports a working public exploit for a vulnerability in the Microsoft JVIEW Profiler (javaprxy.dll) component, an interface to the Microsoft Java Virtual Machine. This vulnerability can be exploited when a user attempts to view an HTML document (e.g., a web page or an HTML email message) that attempts to instantiate the JVIEW Profiler COM object in a certain way.

Successful exploitation could allow an attacker to execute arbitrary code on the user's system with privileges of the user. More information about this vulnerability can be found in the following US−CERT Vulnerability Note:

VU#939605: VIEW Profiler (javaprxy.dll) COM object contains an unspecified vulnerability. Microsoft has published a Security Advisory about this issue and is continuing to investigate the problem. Until a patch is available to address this vulnerability, US−CERT strongly encourages users to review the workarounds section of Vulnerability Note VU#939605.

Current Port Attacks

Top 10 Target Ports	6881 (bittorrent), 445 (microsoft−ds), 1026 (−−−), 135 (epmap), 139 (netbios−ssn), 4672 (eMule), 1433 (ms−sql−s), 65534 (sbininitd), 80 (www), 137 (netbios−ns) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

36. *July 07, KPUA News (HI)* — **Bomb threat at State building on the Big Island of Hawai`i.** The State Building at 75 Aupuni Street in Hilo, HI, was evacuated for about 20 minutes Wednesday, July 6, after state employees received a bomb threat by telephone. At 8:15 a.m., personnel of the State Department of Accounting and General Services received an anonymous phone call in which a male caller said a bomb in the building was set to go off in 25 minutes. The building was evacuated while Hilo police, deputies from the State Sheriff's Office and personnel working inside the building conducted a search. After nothing was found and no injuries were reported in the evacuation, the building was reopened about 9:25 a.m. Source: http://www.kpua.net/news.php?id=5705

37. *July 07, News 8 WMTW (ME)* — **Court complex evacuated after bomb threat.** Business is back to normal at the Portland, ME, courthouse complex. Portland police reported that a bomb

threat on Thursday, July 7, had closed off a number of streets in the vicinity of the complex Thursday morning. Police said that someone called in the threat, citing a specific time of 8:30 a.m. The complex was evacuated until 10 a.m.
Source: http://www.wmtw.com/news/4693141/detail.html

38. *July 07, Associated Press* — **D.C. monument elevator stuck with 35 aboard.** Some 35 people trapped when the Washington Monument's elevator stalled about 120 feet into the ride on Thursday, July 7, were freed by rescuers and walked down to the ground. About 25 people at the top of the monument had to take the stairs down 500 feet, a spokesman for the National Park Service said. A 17−year−old girl was hospitalized with breathing trouble. The monument elevator also got stuck on May 16. Twenty−five people were rescued.
Washington Monument: http://www.nps.gov/wamo/home.htm
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/07/AR2005070701657_pf.html

[Return to top]

General Sector

39. *July 08, The Guardian (UK)* — **Four bombs in 50 minutes−−Britain suffers its worst−ever terror attack.** At least 38 people were killed Thursday, July 7, and more than 700 injured as terrorists struck at the heart of London, causing the biggest loss of life in a terrorist attack on mainland Britain. In a series of coordinated strikes, explosive devices were detonated on three underground trains and a bus travelling through central London during the morning rush hour. Tens of thousands of workers were sent home early as shops and businesses across the London closed−−or failed to open at all−−after the terrorist attacks. The attacks led to events being cancelled, caused road and rail chaos across the capital and disrupted postal services across the country. The Royal Mail said its vehicles had been unable to move in or out of London. Parcelforce was also expecting to be affected. On a normal day a quarter of the country's mail passes through the capital. British Prime Minister Tony Blair said that Britain would not be intimidated by terrorism: "When they try to intimidate us, we will not be intimidated. When they seek to change our country or our way of life by these methods, we will not be changed." Earlier, speaking from Gleneagles, Scotland, site of the G8 summit, the prime minister had said it was "reasonably clear" that the attacks were timed to coincide with the start of the summit. Blair said the summit would continue. By Friday, most of the tube system was running again after security searches overnight, but many trains seemed quieter than usual at the start of the rush hour.
Source: http://www.guardian.co.uk/uk_news/story/0,3604,1523611,00.ht ml and http://www.guardian.co.uk/uk_news/story/0,3604,1523819,00.ht ml

40. *July 08, Bloomberg* — **Hurricane winds reach 135 mph, forcing Florida Keys evacuations.** Hurricane Dennis strengthened overnight into the strongest storm ever this early in the Atlantic hurricane season, forcing mandatory evacuations in parts of the Florida Keys. The hurricane was upgraded to a Category 4 storm on the Saffir−Simpson scale, with maximum sustained winds reaching 135 miles an hour as of 11 p.m. Florida time, the National Hurricane Center said on its Website. Category 4 storms can tear off roofs, destroy mobile homes and require evacuations as far as six miles from the shoreline because of flooding. "This is the first

Category 4 we've ever had in July," said Navy meteorologist Lieutenant Dave Roberts at the Miami−based hurricane center. "It's going to bring storm surges and heavy rain, almost like a curtain−wall effect. That's where most of your damage is going to come from." Florida, which is still recovering and rebuilding after a devastating storm season last year, ordered residents evacuated from the southern Keys, said Kristy Campbell, spokeswoman for the state's emergency operation center. Oil companies have evacuated rigs and production platforms in the Gulf of Mexico east of a line from Cameron, Louisiana, located 80 miles east of the Texas border.
Hurricane map: http://www.nhc.noaa.gov/storm_graphics/AT04/refresh/AL0405W5+gif/211039W_sm.gif
Source: http://www.bloomberg.com/apps/news?pid=10000103&sid=aDWPrynKWK58&refer=us

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

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

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

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

Contact DHS/IAIP

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.