Department of Homeland Security Daily Open Source Infrastructure Report for 21 July 2005

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

Daily Highlights

- USA TODAY reports that the Transportation Security Administration will allow more airports to contract with private companies to administer its Registered Traveler program of expedited security screening of trusted travelers. (See item 11)
- The New York Times reports the New York Metropolitan Transportation Authority has placed the city's underwater tunnels at the top of the list of critical infrastructure, and is exploring methods to increase security. (See item 13)
- Government Computer News reports the Department of Homeland Security is deploying a new data network −− the Homeland Security Information Network−Secret −− to pass classified information to hundreds of state and local officials. (See item 29)

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://esisac.com]

1. *July 20, Associated Press* — **New Yorkers break records for electricity consumption.** New Yorkers coping with temperatures in the 90s and high humidity turned up their air conditioners Tuesday, July 19, and broke records for electricity usage, the Consolidated Edison power company said. By 4 p.m. customers in New York City and Westchester County to the north had

hit an all−time peak, consuming 12,361 megawatts. Statewide, power customers also outdid themselves −− using 31,741 megawatts, according to the New York Independent System Operator organization, which operates the state's power grid. The previous records for the city and the state were set on August 9, 2001.
Source: http://www.usatoday.com/weather/stormcenter/2005−07−20−nyc−h eat_x.htm

2. *July 19, Associated Press* — **Indian Point siren system deactivated after power loss.** The sirens that are meant to warn thousands of people of an emergency at the Indian Point nuclear power plants, located in Buchanan, NY, stood useless for nearly six hours Tuesday, July 19, when power was lost to a signal transmitter and the failure went undiscovered. There was no emergency, and the 156 sirens were not needed during the outage, which lasted from 2 a.m. to 7:45 a.m. Larry Gottlieb, a spokesperson for Indian Point owner Entergy Nuclear Northeast, said the cause of the outage was not known but there was "no evidence of sabotage." The sirens are meant to alert residents within 10 miles of the plants to tune in broadcasts about an emergency. Nuclear Regulatory Commission spokesperson Neil Sheehan said the commission would investigate.
Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−ind ianpoint0719jul19,0,4670602.story?coll=ny−region−apnewyork

3. *July 18, Reuters* — **U.S. transport official warns of brownout risk.** A top U.S. transportation official warned on Monday, July 18, that coal shortages caused by damage to railroad tracks in the primary U.S. coal−mining region could trigger electrical brownouts this summer in pockets of the country. In an interview, the chairman of the Surface Transportation Board, Roger Nober, said brownouts −− a potentially disruptive dip in electrical voltage on the grid −− were a possibility as the nation heads into a period of peak electricity consumption. "There is the possibility, of course, that individual utilities who were low on stockpiles for whatever reason may find themselves short now," he said. A combination of heavy precipitation and built−up coal dust has been blamed for May's two derailments on a line jointly operated by Union Pacific and Burlington Northern Santa Fe Corp. in the Powder River Basin of Wyoming and Montana. Utilities have begun reporting shortages of the raw material for their coal−fired power plants. Coal accounts for more than half of all the power generation in the United States, experts say, with much of it coming from the basin. The peak season for electricity consumption is typically from June through September, when hot summer temperatures boost demand for air conditioning.
Source: http://today.reuters.com/investing/financeArticle.aspx?type= bondsNews&storyID=2005−07−18T233259Z_01_N18188282_RTRIDST_0_ ENERGY−BROWNOUTS−UPDATE−3.XML

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *July 19, Federal Computer Week* — **Chinese military targeting defense technology.** Department of Defense (DoD) officials acknowledged in a new report that the Chinese military is developing sophisticated communications systems and computer network operations. The People's Liberation Army is developing modern, integrated command, control, communications, computers, intelligence, surveillance and reconnaissance systems, the DoD report states. The Chinese military is bolstering its ability for computer network attacks, defense, and exploitation, according to "Annual Report to Congress: The Military Power of the People's Republic of China 2005." "The People's Liberation Army has likely established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics to protect friendly computer systems and networks," according to the report. DoD officials said the Chinese military believes the use of information technology and electronic warfare weapons can increase its effectiveness early in a battle. The DoD report on China's increasing military capability including its emphasis on IT follows recent statements from department and military officials that U.S. military systems are increasingly under attack from adversaries.
   Annual Report to Congress: The Military Power of the People's Republic of China 2005: http://www.defenselink.mil/news/Jul2005/d20050719china.pdf
   Source: http://www.fcw.com/article89622−07−19−05−Web

[Return to top]

Banking and Finance Sector

5. *July 20, Arizona Daily Star* — **Officials break up identity theft racket.** Six people in Arizona were arrested Tuesday, July 19, and accused of participating in an identity theft ring that included a state agency and a county court among its victims. Detectives from the Pima County Sheriff's Department and the Sahuarita Police Department said they hope to make seven additional arrests and continue the investigation. The group stole bank−account information from the Clerk of Pima County Superior Court, the Arizona Department of Economic Security and five people, created counterfeit checks using a computer and cashed at least $20,000 at Sahuarita−area stores, said Detective Pat Willson of the Sheriff's Department fraud division. She wouldn't say how they stole the account numbers or how they spent the money. Willson said the investigation into extensive fraud activity turned up methamphetamine and marijuana in three houses authorities searched.
   Source: http://www.dailystar.com/dailystar/allheadlines/84931.php

6. *July 19, Reuters* — **Hackers get into university database.** A University of Southern California (USC) database containing about 270,000 records of past applicants was hacked last month, officials said on Tuesday, July 19. The breach of the university's online application database exposed dozens of records, which included names and Social Security numbers, to unauthorized individuals, said Katharine Harrington, USC dean of admissions and financial aid. Harrington could not be more specific about the number of people whose personal data may have been viewed by the hacker or hackers, nor about what the motivation had been for the computer break−in. "There was not a sufficiently precise tracking capability," Harrington said, but added that the hackers had not been able to access multiple records at once. Records were also only able to be viewed at random, she said. "We are quite confident that there was no

massive downloading of data," Harrington said. USC learned of the breach June 20 when it was tipped off by a journalist, Harrington said. It has since shut down the Website and has notified people whose names and Social Security numbers were in the database that was breached. The site will be back up once new security measures are taken, the university said in a written statement.
Source: http://news.com.com/Hackers+get+into+USC+database/2100−7349_3−5795373.html?tag=nefd.top

[Return to top]

Transportation and Border Security Sector

7. *July 20, Wireless Week* — **Last two New York tunnels get wireless service back.** Wireless service was restored on Tuesday, July 19, to the two New York tunnels that had been without wireless service since the July 7 attacks on the London transportation system. The Port Authority of New York and New Jersey turned the power back on to transmission facilities in the Holland and Lincoln tunnels after security consultations, a Port Authority spokesperson said. Service to all four major tunnel arteries leading into and out of Manhattan had been shut off July 7 after subway tunnels in London were bombed. The Metropolitan Transit Authority, which owns the Midtown and Brooklyn tunnels, turned power in those tunnels back on five days after it was turned it off, but the Port Authority held out, citing security concerns. The decision to cut off power was made by the owners of the tunnels as a precautionary measure; cell phones had been used to detonate explosives in attacks last year on the Madrid subway system.
Source: http://www.wirelessweek.com/article/CA627012.html

8. *July 20, Department of Transportation* — **Grant seeks greater safety for California Metrolink passengers.** The federal government wants to know if it is possible to restrict vehicle access to two Metrolink commuter train lines as a way to improve safety on routes that run from Los Angeles to Symar and Chatsworth, it was announced on Wednesday, July 20. The Federal Railroad Administration (FRA) said it would give Metrolink $250,000 to study a "sealed corridor" concept for its Antelope Valley and Ventura County lines. The study will evaluate whether it is possible to reduce or eliminate the chance of cars crossing into the path of trains. In a sealed corridor, approach, passenger and freight rail operators work with state transportation and local officials to analyze safety at all railroad crossings along a particular rail line. The purpose of the assessment is to decide which grade crossings should receive safety improvements or be permanently closed. The study will be modeled on the successful efforts of the North Carolina Department of Transportation to implement a sealed corridor between Charlotte and Raleigh. To date along that line, safety upgrades have been made at 67 crossings and 64 public and private crossings have been closed, with improvements at over 100 others still in various stages of project development.
Source: http://www.dot.gov/affairs/fra1805.htm

9. *July 20, Department of Transportation* — **DOT to study safer seats, tables for commuter trains.** The Department of Transportation's (DOT) Research and Innovative Technology Administration (RITA) on Wednesday, July 20, launched a new project to make seats and tables on commuter trains safer. Working with the Federal Railroad Administration (FRA),

RITA's Volpe National Transportation Systems Center has awarded two contracts worth $850,000 to a Massachusetts−based technology firm to develop a safer passenger seat and worktable that will reduce injuries and improve the ability of passengers to safely exit a train following a collision. The project supports several rail safety initiatives being conducted jointly by the FRA and RITA's Volpe Center, including ongoing research in the areas of crashworthiness, emergency evacuation, grade crossing and safety decision−making. The project plans to design a worktable that will absorb energy upon impact and reduce the risk of head, chest, abdomen and leg injuries. In addition, improved three−person seats will be developed to reduce the risk of head, chest, and leg injuries. Since 1992, Volpe Center and FRA have focused on both passenger and freight structural crashworthiness and occupant protection. The research has found that it is possible to make passenger train travel safer using a combination of these two elements.
Source: http://www.dot.gov/affairs/rita805.htm

10. *July 20, Reuters* — **American Airlines, Continental beat forecasts on strong traffic.** American Airlines and Continental Airlines posted much better−than−forecast quarterly earnings Wednesday, July 20, offering a glimmer of hope for a recovery in the loss−plagued U.S. airline industry. The profits follow a string of quarterly losses by traditional U.S. carriers, which have struggled to find ways to pass on record fuel costs to passengers amid fierce competition from low−cost rivals. American Airlines' parent company AMR said second−quarter net profit rose to $58 million, or 30 cents a share, from $6 million, or 3 cents a share, a year earlier. The No. 1 U.S. carrier said it was the first time in 17 quarters it had posted a profit without the benefit of one−off gains. Continental, the No. 5 U.S. airline, reported a net profit of $100 million, or $1.26 a share, compared with a loss of $17 million, or 26 cents a share, in the year−ago period.
Source: http://www.usatoday.com/travel/news/2005−07−20−amer−cont−pro fit_x.htm

11. *July 20, USA TODAY* — **Companies get approval to run security screening.** The government will allow more airports to contract with private companies to administer its program of expedited security screening of trusted travelers. On Tuesday, July 19, Justin Oberman, Transportation Security Administration assistant administrator, said in comments at the launch of Orlando, FL's Registered Traveler program, the first operated by a private company, that the government's Registered Traveler program will "move a lot faster" with companies −− not the government −− running it. Registered Traveler allows people who have passed background checks to enter a special line at airport checkpoints. They go through a metal detector but are exempt from additional screening unless they trigger an alarm. A year−old TSA test of Registered Traveler has been limited to 10,000 enrollees at five airports −− Boston, Washington Reagan National, Houston Bush, Minneapolis and Los Angeles. The TSA had been considering whether it should continue to run the program or turn it over to airports and airlines that team with marketing and technology companies.
Source: http://www.usatoday.com/travel/news/2005−07−19−registered−us at_x.htm

12. *July 20, USA TODAY* — **Cities look for ways to secure rails.** Subway riders may face random police checks of their bags under a security measure being considered in the nation's capital. No decision has been made on the idea for the District's 106−mile Metrorail system, and the logistics would be difficult. But "it would be another tool in our security toolbox," says Washington Metropolitan Area Transit Authority spokesperson Lisa Farbstein. The possibility

is one of many ideas being floated in Washington, DC, and elsewhere while the terrorist threat level for transit systems remains at "high" after the July 7 terrorist suicide bombings in London's underground rail tunnels. Many of the U.S.'s commuter rail and subway systems are much more difficult to secure than airports because they are vast and open. Several cities have bolstered security by adding to what's already available: more cameras, more bomb−sniffing dogs and more announcements reminding people to report suspicious behavior and packages. Last year, after terrorists bombed rush−hour commuter trains in Madrid, the Department of Homeland Security tested explosive detection equipment on some rail passengers at stations in Maryland and Washington, DC. But because subway systems have so many entrances and exits, it would be impossible to deploy and staff enough of the machines to secure the system.
Source: http://www.usatoday.com/news/nation/2005−07−19−cities−secure −rails_x.htm

13. *July 20, New York Times* — **Security concerns for underwater tunnels.** Hours after the London subway and bus bombings on July 7, New York City's police commissioner, Raymond W. Kelly, announced that officers would be posted immediately at the entrances to all 14 of the city's underwater subway tunnels. The action underscored concerns about the tunnels, and exposed this reality: for most of the time since 9/11, nearly half of the tunnels have not been continuously guarded by the police. The question of how best to safeguard the tunnels is among the most vexing for the police and transportation officials struggling to address the many security challenges posed by the country's busiest mass transit system. One vulnerability assessment after another conducted since September 11, 2001, by or on behalf of the Metropolitan Transportation Authority has placed the underwater tunnels at the top of the list of critical infrastructure. The 14 tunnels form a vital network and are the product of varied construction methods spanning decades. The authorities have so far focused their efforts on trying to control access to the tunnels, while exploring longer−term improvements like using new synthetic materials to buffer tunnels against an attack. The current 24−hour coverage at all 14 tunnels will continue at least as long as the country's mass transit systems remain in a state of high alert, chief police spokesperson, Paul J. Browne said.
Source: http://www.nytimes.com/2005/07/20/nyregion/20tunnels.html?or ef=login&oref=login

[Return to top]

Postal and Shipping Sector

14. *July 20, Quad City Times (IA)* — **Illinois city installs anthrax detection system.** The Milan, IL, processing and distribution facility unveiled sophisticated new equipment Tuesday, July 19, that tests mail for anthrax and sounds an alarm if it is detected. The Milan location, which employs 240 people, sorts through 1.5 million pieces of mail per night. It handles mail for 140 post offices from as far south as the Missouri border to Iowa City and north to Clinton, Iowa. The anthrax−detection system uses sophisticated DNA matching to detect the presence of the bacteria in the mail. It continuously collects air samples from mail−canceling equipment as it operates. The airborne particles are absorbed by a sterile water base, which creates a liquid sample that can be tested. The liquid sample is collected in a cartridge. The detection equipment consists of an air collection hood, a cabinet where the collection and analysis devices are housed, a local computer network connection and a site controller. It takes about 90 minutes to detect the anthrax −− one hour for the air collection process and 30 minutes to test the sample. Since air sample collections are continuous, and test results will be known every hour after the

initial test. That gives the Postal Service time to recall trucks of mail, if necessary.
Source: http://www.qctimes.net/articles/2005/07/20/news/local/doc42dde2ec05fb1032598598.txt

[Return to top]

Agriculture Sector

15. *July 21, The Ledger (FL)* — **Citrus canker spreads North.** Confirmed outbreaks of citrus canker on five residential properties in Clay County, FL, just south of Jacksonville, FL, mark the most northward spread of the bacterial disease in Florida since its 1995 reappearance near Miami. An Orange Park, FL, resident reported apparent symptoms of the disease on his grapefruit tree, according to a press statement from the Florida Department of Agriculture and Consumer Services. Officials subsequently confirmed the tree had canker and found six other infected trees on four properties nearby. The outbreaks likely sprang from movement of infected plant material, the statement said.
Source: http://www.theledger.com/apps/pbcs.dll/article?AID=/20050720/NEWS/507200380/1001/BUSINESS

16. *July 20, New Mexico Business Weekly* — **Federal government halts New Mexico's bovine tuberculosis testing requirement.** In a move that could mean big savings for the State's cattle producers, the Federal government has approved a plan developed by the New Mexico Livestock Board to help the state's cattle and dairy industry gain back its bovine tuberculosis (TB) free status, New Mexico's Democratic U.S. Senator Jeff Bingaman announced on Wednesday, July 20. New Mexico lost its TB−free status in 2003 after several dairy cows were diagnosed with the disease and the loss of the status required all cattle be tested before they are shipped outside the State. Under the New Mexico Livestock Board plan, which has been approved by the U.S. Department of Agriculture, only those animals in the small area in Roosevelt County, NM, where the bovine TB was diagnosed will require additional testing and surveillance.
Source: http://albuquerque.bizjournals.com/albuquerque/stories/2005/07/18/daily10.html?jst=b_ln_hl

17. *July 20, AgProfessional* — **University of Illinois advises precautions against nitrate toxicosis.** According to a University of Illinois Extension dairy veterinarian Dick Wallace, "Producers need to take precautions as they attempt to locate alternate forage sources or consider chopping drought−stressed corn...Several crop species can accumulate nitrates but especially grasses such as corn, oats, wheat, barley and sorghum." Chopped drought−stressed grass crops are a common source of nitrate toxicity on dairy operations. Most plants extract nitrogen from the soil in the form of nitrates. Nitrates accumulate in plants when the rate of nitrate uptake increases or the reduction of nitrates to nitrites decreases. Increased application of nitrogen fertilizers may increase uptake. According to Wallace, when grass crops are stressed, such as by drought conditions, the concentration of nitrates in plant tissues increases because the ability of the plant to reduce nitrates to nitrites is impaired. Rumen microorganisms rapidly reduce nitrate to nitrite and when unconditioned cattle consume plants containing high levels of nitrates, the nitrate to nitrite conversion exceeds the ability of the rumen microbes to convert nitrites to ammonia. "Blood levels of nitrites increase and alter the hemoglobin in red

blood cells to produce methemoglobin. Chopped drought−stressed grass crops are a common source of nitrate toxicity on dairy operations.
Source: http://www.agprofessional.com/show_story.php?id=34103

18. *July 20, Iowa Ag Connection* — **Actions teams created to monitor, respond to drought.** As hot and dry conditions persist in parts of major food−producing regions, Agriculture Secretary Mike Johanns and Interior Secretary Gale A. Norton have activated Interagency Drought Action Teams. These teams will coordinate drought relief in Western states facing the greatest potential water shortages this summer. Although both agencies use different approaches and tools when addressing drought conditions, the teams are working together and with local officials in Washington, Oregon, Idaho, Montana and other states as drought concerns are identified.
Source: http://www.iowaagconnection.com/story−state.cfm?Id=601&yr=20 05

19. *July 20, Northeast Mississippi Daily Journal* — **Soybean rust found in Mississippi.** Researchers in the State's southeastern corner discovered Mississippi's first case this year of Asian soybean rust. Asian soybean rust appeared on a plant in George County, MS, state Agriculture Commissioner Lester Spell announced Tuesday, July 19. And though the fungal disease has never touched Northeast Mississippi soybeans, many growers say it's only a matter of time. Soybean rust attacks a plant's foliage and causes the leaves to drop early. This interferes with the pods' development and can lessen a farmers' yield at harvest. The only way to prevent or fight the disease is by spraying crops with fungicide. Mississippi farmers −− who collectively planted about 1.6 million acres of soybeans this year −− have been encouraged to monitor their fields and report any suspicious findings to the extension service.
Source: http://www.djournal.com/pages/story.asp?ID=197767&pub=1&div= News

[Return to top]

Food Sector

20. *July 20, Independent (United Kingdom)* — **Bovine spongiform encephalopathy cluster triggers fears over contaminated feed.** A cluster of bovine spongiform encephalopathy (BSE) is being investigated by scientists who fear that contaminated feed is still being given to British cattle. The cluster involving three young cows born long after the 1996 ban on contaminated feed is believed to have been found on a dairy farm in England. It is the second such cluster of young BSE cases. The first occurred on a farm in Wales and it too involved three young cattle that were born many years after the United Kingdom banned all animal feed that could be contaminated with BSE. Scientists said the occurrence of a second cluster of BSE in young cattle strongly suggested that the cases were not a statistical fluke and that contaminated feed had caused the outbreaks. So far there have been 106 confirmed cases of BSE in cattle born since the 1996 "reinforced feed ban" after which, in theory, no newborn calf should have been exposed to the infectious agent responsible for the disease. However, of the 85 confirmed cases of BSE reported this year, 13 of them were in cattle born after the 1996 feed ban, which should have eliminated the possibility of new infections in Britain.
Source: http://news.independent.co.uk/uk/environment/article300340.e ce

21. *July 19, United States Department of Agriculture* — **Chile opens borders to U.S. beef.** Agriculture Secretary Mike Johanns on Tuesday, July 19, announced that Chile is lifting its ban on U.S. beef and beef products from animals less than 30 months of age. In 2003, the United States exported $5.3 million worth of beef and beef products to Chile. Chile imposed a ban on U.S. beef and beef products on December 24, 2003.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2005/07/0270.xml

22. *July 18, Food Navigator* — **Russian scientists design new preservative.** Food scientists in Russia have developed a new, safer preservative for meat and fish that they claim improves resistance to harmful bacteria and could extend shelf life by up to 50 percent. Specialists from the Nijnyi Novgorod Fat−and−Oil factory (NMJK), together with Russian Scientific Research Institute for Food Aromatisers and Acids, designed the preservative known as Dilactin−S and the technology to manufacture it. Dilactin−S is claimed to have a unique combination of physical, chemical, biochemical, technological properties, which increase a product's resistance to microbes. It also increases shelf life by between 30 and 50 per cent by slowing down the oxidation process. The new ingredient is also capable of saving time during production, increasing a product's moisture retention, improving pH levels in a product and cutting the amount of nitrate present in boiled sausages.
Source: http://www.foodnavigator.com/news/news−ng.asp?n=61349−russian−scientists−design

[Return to top]

Water Sector

23. *July 20, Daily News (CA)* — **Water security measures approved.** Security measures expected to cost more than $1.4 million will be installed around wells and water−treatment facilities that supply tens of thousands of Antelope Valley, CA, homes. Los Angeles County supervisors on Tuesday, July 19, approved spending the money to help protect Los Angeles County Waterworks District facilities in the Antelope Valley against terrorist attack. Work on the project is scheduled to begin in October and be completed by June 2006. The board, in approving the project, acted as the governing body of the county Waterworks District No. 40, which covers much but not all of Lancaster and most of west Palmdale. The waterworks district serves more than 50,600 homes and businesses in much of Lancaster and west Palmdale, as well as about 7,200 customers in areas of Lake Los Angeles, Pearblossom and other parts of the valley. The Antelope Valley waterworks district will be the first to receive security improvements among the sites overseen by the county public works department. The project calls for installing remote cameras, closed circuit television monitors, motion sensors, and digital video recorders at nine locations. The project also will include the construction of concrete block walls, fences, gates, bars for windows, and other work.
Source: http://www.dailynews.com/Stories/0,1413,200~20943~2972141,00 .html

24. *July 18, Rocky Mountain News (CO)* — **Staff shortage threatens safety of Colorado's future supply.** Colorado's system to oversee the safety of drinking water is significantly understaffed, threatening the integrity of a program designed to protect public health. The U.S. Environmental Protection Agency (EPA), in a review of the state health department's drinking

water program, repeatedly warned that staffing levels far below national standards spread supervisors too thin and could delay important new regulatory initiatives. "The drinking water program must be able to respond to . . . emergencies, maintain (its) basic program and be able to move the program forward in a comprehensive manner to . . . ensure the safety of drinking water," the report said. "The current level of resources simply does not make this possible, and this course of action is not without its risks to the public health." The EPA's emphasis on staffing shortfalls marked the latest red flag over personnel levels at Colorado's Water Quality Control Division. A draft report by the division itself last year found that the state's water pollution watchdog agency was staffed 40 percent below states of comparable size and responsibilities, and could be at risk of takeover by the federal government. And last month, two members of the state's governor−appointed Water Quality Control Commission raised concerns about a lack of personnel in the division.
Source: http://rockymountainnews.com/drmn/state/article/0,1299,DRMN_21_3934747,00.html

25. *July 18, Yahoo Finance* — **General Electric, Gen−Probe form alliance.** General Electric Infrastructure, Water & Process Technologies, a unit of General Electric Company (GE), and Gen−Probe announced Monday, July 18, that the two companies will work together on an exclusive basis to develop, manufacture, and commercialize nucleic acid testing (NAT) technologies that are designed to detect the unique genetic sequences of microorganisms in selected water applications. Worldwide, 1.2 billion people do not have access to safe, usable water daily, and five million people die each year from waterborne diseases. The most common and pervasive water risks are caused by infectious diseases such as pathogenic bacteria, viruses, and protozoan parasites. People are introduced to these microorganisms through contaminated drinking water, irrigation, aerosols, and washing or bathing. The companies estimate that more than one billion industrial microbiology tests are conducted annually around the world. Roughly three−quarters of these tests are conducted using culture methods that cannot deliver results as rapidly as NAT technologies.
Source: http://www.sddt.com/News/article.cfm?SourceCode=20050718czf

[Return to top]

Public Health Sector

26. *July 20, Associated Press* — **World Health Organization presses China over bird flu samples.** China hasn't responded to urgent appeals by the World Health Organization (WHO) to share data about wild birds killed by avian flu, an official said Wednesday, July 20, as fears mounted that other birds might spread the disease when they migrate to other countries. Authorities also haven't responded to a WHO request to be allowed to visit the Xinjiang region in China's northwest, where there have been reports of a bird flu outbreak along the border with Kazakhstan, said Roy Wadia, a spokesperson for WHO's Beijing office. Chinese authorities have yet to release samples gathered in the western province of Qinghai, where at least 6,000 migratory birds have died, Wadia said. "It would be useful if information on the virus was shared with the international agencies concerning bird flu, or if it were deposited at gene banks as per the usual procedures in these cases," Wadia said. China's failure to respond to foreign appeals for cooperation has prompted fears that the outbreak might be bigger and more dangerous than reported. Wadia said the sequencing of the virus' DNA was "very important" because it could help experts confirm whether the strain affecting birds in Qinghai was new or

an old one with minor mutations. Chinese tests have confirmed that it is a strain of H5N1. Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/07/20/AR2005072000158.html

27. *July 20, Agence France Presse* — **Indonesia confirms first human deaths from bird flu.** Indonesia confirmed its first human deaths from bird flu, saying tests had shown a man and his two daughters who died this month had a deadly strain of the disease. "It's confirmed. They died of the conventional bird flu virus which does not transmit from humans to humans," Health Minister Siti Fadillah Supari told Agence France Presse. She said the tests done in Hong Kong were based on specimens from the father and one of the daughters, but it could be concluded that all three had died of the deadly H5N1 strain of bird flu. She said it was not known when and where the 38−year−old man, Iwan Siswara Rafei, and his two young daughters −− one and nine years old −− had been infected. But she added that the authorities believed the three had contracted the disease at about the same time. The family's house in Tangerang district, just southwest of Jakarta, is far from areas were there are bird flu outbreaks, she said. Rafei and his daughters died within days of each other in hospital in the first half of July after suffering from severe pneumonia.
Source: http://news.yahoo.com/s/afp/20050720/hl_afp/healthindonesiaf lu_050720104258

28. *July 19, Associated Press* — **Hamster with deadly virus linked to Ohio distribution center.** A pet hamster that carried a virus blamed in the deaths of three New England organ recipients came from an Ohio distribution center that sends hamsters to pet stores throughout the East Coast, a state agriculture official said Tuesday, July 19. Ohio's Agriculture Department along with federal health investigators quarantined the distribution center Monday, July 18, and began testing animals for the virus. "We don't know whether the disease is there or not," said LeeAnne Mizer, a spokesperson for the Ohio Department of Agriculture. "It's a potential threat." The U.S. Centers for Disease Control and Prevention informed state agriculture officials that it traced the hamster's origin to Mid−South Distributors of Ohio, which is in Norwich, Mizer said. The virus, lymphocytic choriomeningitis, is uncommon and rarely fatal to humans. It can be dangerous, though, to anyone with weak immune systems. Health officials say the organ donor caught the virus from a pet hamster, and it was transmitted to the organ recipients whose weakened immune systems put them at higher risk. A doctor at a Rhode Island Hospital discovered the infection in April, when two of her kidney transplant patients developed flu−like symptoms. One of the patients died. Two patients in Massachusetts also died in April within a few weeks of their transplants.
Source: http://news.bostonherald.com/localRegional/view.bg?articleid =94482

[Return to top]

Government Sector

29. *July 20, Government Computer News* — **DHS launches state, local network.** The Department of Homeland Security (DHS) is deploying a new “secret” data network to pass classified information to hundreds of state and local officials, DHS officers said at a congressional hearing on Wednesday, July 20. The Homeland Security Information Network−Secret (HSIN−Secret) is an “immediate, inexpensive and temporary approach to reach state and local homeland security and law enforcement sites that can receive secret−level information,”

Matthew Broderick, director of the Homeland Security Operations Center, said in testimony on Wednesday, to the House Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. The new network is operating and will continue to do so until the DHS secret−level backbone called the Homeland Security Data Network is initiated in fiscal 2007, Broderick said. The HSIN−Secret classified network is being deployed and tested at 50 state emergency operations centers and 18 additional state and local law enforcement sites. In addition to the secret−level network, HSIN's other networks include a common portal for all state and local governments; a portal for law enforcement agencies with intelligence analysis units and law−enforcement agencies that deal with sensitive data; emergency operations centers; an international link for rapid dialogue with the United Kingdom, Canada and Australia during a crisis; and the Computer Emergency Response Team for cybersecurity.
House Testimony: http://hsc.house.gov/release.cfm?id=394
Source: http://www.gcn.com/vol1_no1/daily−updates/36443−1.html

[Return to top]

Emergency Services Sector

30. *July 21, The Age (Australia)* — **Mock rail attack planned in Australian city.** A mock attack on Melbourne's City Loop rail line in Australia will be carried out in coming months as the Victorian Government intensifies efforts to prepare the state for the possibility of a terrorist strike. The exercise was part of measures that Premier Steve Bracks outlined to Parliament yesterday in response to the London bombings. Bracks said the Government would update and extend closed−circuit television on trains and at some station car parks, and look at extending an emergency warning system, about to be tested in the Yarra Ranges and Northern Grampians, which would send a recorded message to home phones informing people of danger. The mock attack is likely to occur on a weekend, with Victorians given warning to ensure there is no panic.
Source: http://www.theage.com.au/news/war−on−terror/mock−rail−attack−plan−as−city−prepares−for−terror/2005/07/20/1121539032244.h tml?oneclick=true

31. *July 20, Green Bay Press−Gazette (WI)* — **Exercise to test readiness of local health officials.** Public health officials will participate Thursday, July 21, in exercises simulating reaction to a bio−terrorist strike. The exercises simulating a human exposure to anthrax will take place at the regional U.S. Postal Service (USPS) Processing and Distribution Center in Green Bay, WI. Participants include public health officials representing eight counties and the city of De Pere. Close to 150 people are expected to attend the clinic that will test the response to a bio−terrorism event using the new USPS biohazard detection system, according to Cullen Peltier, Emergency Management Director for Brown County. Terri Michlig, a customer relations coordinator at the Green Bay Postal Service, said all the mail processing plants across the country have already or will have this detection system installed to increase security for the country's top mail distributor. According to Steve Johnson, the bio−terrorism grant coordinator for Oneida Community Health Services and the Brown County and De Pere health departments, anthrax may be an unlikely agent to appear in Northeastern Wisconsin, but if the health departments are prepared for it, they will be prepared for other, more likely epidemics, such as influenza or SARS.

Source: http://www.greenbaypressgazette.com/news/archive/local_21811 607.shtml

32. *July 19, SitNews (AK)* — **Training exercise will join local, state and federal agencies.** Residents in Ketchikan, AK, will see an increase in emergency response and law enforcement activity in the coming weeks as Ketchikan prepares for Alaska Shield/Northern Edge 2005, August 15−19. City of Ketchikan Public Safety Director Rich Leipfert said that Ketchikan is one of 13 communities in the state that will test its abilities to respond to a terrorist incident during the month of August. He anticipates locally, approximately 400 people representing more than 40 local, state and federal organizations will participate in this large−scale training exercise. Scenarios will not only evaluate the strengths and weaknesses of these agencies' emergency and law enforcement personnel, but the readiness of area government officials to respond to a terrorist act or threat. In addition to the August 15, all−day tabletop exercise, there will be a hazardous materials drill at Ketchikan Charter School on August 16 involving an entry team, sample collection, evidence collection, and decontamination of response personnel. Finally, on August 18, a full−scale mock catastrophe at a "still undisclosed location" will challenge participants' resources and skills to help guarantee our community will be prepared for large−scale events, no matter what the cause.
Source: http://www.sitnews.us/0705news/071905/071905_ak_shield_n_edg e.html

[Return to top]

Information Technology and Telecommunications Sector

33. *July 20, Government Computer News* — **DHS to mount major IT security exercise.** The Department of Homeland Security plans to conduct a major cybersecurity preparedness and response exercise to be called Cyber Storm in November, a department official said in congressional testimony Tuesday, July 19. Andy Purdy, acting director of DHS' National Cyber Security Division (NCSD), described Cyber Storm as "a national exercise" during a hearing of the Senate Homeland Security and Governmental Affairs Subcommittee on Federal Financial Management, Government Information and International Security. According to written testimony Purdy presented, the division has worked with the Justice and Defense departments to help form the National Cyber Response Coordination Group (NCRCG). "The NCRCG has developed a concept of operations for national cyber incident response that will be examined in the National Cyber Exercise, Cyber Storm, to be conducted by NCSD in November 2005 with public and private−sector stakeholders."
Securing Cyberspace: Efforts to Protect National Information Infrastructures Continue to Face Challenges: http://hsgac.senate.gov/index.cfm?Fuseaction=Hearings.Detail &HearingID=261
Source: http://www.gcn.com/vol1_no1/daily−updates/36434−1.html

34. *July 19, Government Accountability Office* — **GAO−05−827T: Critical Infrastructure Protection: Challenges in Addressing Cybersecurity (Testimony).** The Homeland Security Act of 2002 and federal policy established the Department of Homeland Security (DHS) as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures. GAO was asked to summarize previous work, focusing on (1) DHS's responsibilities for cybersecurity−related critical infrastructure protection (CIP), (2) the status of the department's efforts to fulfill these responsibilities, (3) the challenges it faces in fulfilling its cybersecurity responsibilities, and (4) recommendations GAO has made to improve

cybersecurity of our nation's critical infrastructure. While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the 13 responsibilities, and much work remains ahead. The department established the US−CERT as a public/private partnership to make cybersecurity a coordinated national effort, and it established forums to build greater trust and information sharing among federal officials with information security responsibilities and law enforcement entities. However, DHS has not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions.
Highlights: http://www.gao.gov/highlights/d05827thigh.pdf
Source: http://www.gao.gov/new.items/d05827t.pdf

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 noted that a number of new exploits came out this weekend. If you are using applications vulnerable to these exploits, ensure you patch and update your software. A new Sybase vulnerability was reported which could give a remote attacker the capability to execute code with administrator privileges. Microsoft has been aware of and working on fixing a Remote Desktop Protocol (RDP) vulnerability since May, but has not released a fix yet. Some scanning of Port 3389, associated with RDP, was noted over the weekend. We recommend you take one or more of the actions recommended by Microsoft (see below) to mitigate this vulnerability.

Current Port Attacks

Top 10 Target Ports	6881 (bittorrent), 1026 (−−−), 445 (microsoft−ds), 27015 (halflife), 139 (netbios−ssn), 1433 (ms−sql−s), 135 (epmap), 6889 (−−−), 80 (www), 4672 (eMule) 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