Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 07 July 2005

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

Daily Highlights

- Bloomberg reports Tropical Storm Cindy has left more than 318,000 people along the Louisiana coast without power; in addition, the Louisiana Offshore Oil Port, the largest U.S. import terminal, has stopped unloading tankers. (See item 2)
- USA TODAY reports maritime security experts say that the Coast Guard's ships, planes, and helicopters are breaking down at record rates, which may threaten the service's ability to carry out its post−9/11 mission of protecting ports and waterways against terrorism. (See item 9)
- The Brattleboro Reformer reports evacuation plans may not work for childcare centers since there is no centralized transportation system and children are usually dropped off by their parents. (See item 25)

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 06, Reuters* — **Louisiana refineries hit by outages.** Electrical power outages in the New Orleans area caused by Tropical Storm Cindy affected at least two Louisiana refineries on Wednesday, July 6, according to company spokespersons. Operations at Chalmette Refining LLC's 187,000 barrel−per−day (bpd) refinery in Chalmette were disrupted early Wednesday morning, said spokesperson Nora Scheller. Electrical power was restored at Murphy Oil's

120,000 bpd refinery in Meraux, a company spokesperson said. The company was working to return the refinery to full production, said Mindy West, director of investor relations. An estimate of when the refinery would return to full production was not available.
Source: http://news.yahoo.com/news?tmpl=story&u=/nm/20050706/bs_nm/energy_storm_refineries_dc_1

2. *July 06, Bloomberg* — **Cindy hits Louisiana gulf coast as Tropical Storm Dennis looms.** Tropical Storm Cindy left more than 318,000 people along the Louisiana coast without power, as Dennis headed toward and threatened to become the earliest hurricane to form in the Atlantic Ocean this year. Oil and natural gas producers evacuated workers and cut output in the Gulf of Mexico on Tuesday, July 5, because of Cindy, and the Louisiana Offshore Oil Port, the largest U.S. import terminal, stopped unloading tankers. Cindy knocked out power to homes and businesses in parts of Alabama, Florida, Louisiana and Mississippi, including about 278,000 in the New Orleans area, utilities said. The storm flooded homes and downed trees and power lines in several parishes in Louisiana. Mississippi Governor Haley Barbour declared a state of emergency in areas affected by the storm.
Source: http://www.bloomberg.com/apps/news?pid=10000086&sid=aqmZTgUb hg.A

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *July 06, SecurityFocus* — **Flawed university admissions site allowed access to applicant data.** A programming error in the University of Southern California's (USC) online system for accepting applications from prospective students left the personal information of as many as 320,000 users publicly accessible, school officials confirmed on Tuesday, July 5. The flaw could have allowed an attacker to send commands to the database that powered the site by using the user name and password text boxes. USC's Information Services Division confirmed the problem and shuttered the site this week as a precaution. The university believes only a handful of records were actually accessed and plans to contact each person. SecurityFocus notified the university of the issue two weeks ago after being tipped off by the discoverer, who claimed to be a security−savvy student who found the flaw during the process of applying to USC. The university initially removed the log−in functionality from the site for several days, but allowed applicants to log in for most of last week. USC completely blocked access to the site this week.
Source: http://securityfocus.com/news/11239

4. *July 06, Associated Press* — **New Vermont law shields against identity theft.** Vermonters who become the victims of identity theft can stop the financial bleeding by putting a freeze on their credit reports, under a new state law. "Identity theft is a big problem, getting bigger, both here in Vermont and nationally," said Attorney General William Sorrell, whose office pushed for the law as part of a package of identity theft protections last year. Experts say consumers are largely left to themselves to clean up the mess, a process that can take hundreds of hours of work and cost up to $1,200. "One of the biggest headaches that identity theft victims have to deal with is cleaning up the damage done to their credit records when crooks open new accounts in their names," said Susanna Montezemolo, a policy analyst with Consumers Union. She said the freeze that Vermont's new law allows consumers to place on their credit can limit the damage to their credit records. When a consumer invokes a credit freeze, a company looking to extend credit to that consumer is blocked from running a check with the three major credit rating companies that operate in the United States.
   Source: http://www.timesargus.com/apps/pbcs.dll/article?AID=/20050706/NEWS/507060324/1003

5. *July 05, TheWGALChannel.com (PA)* — **Phishing scam dupes bank's customers.** Customers of one of the Susquehanna Valley, Pennsylvania's largest banks have been targeted in a phishing scam, with a few people having been victimized. Customers of Fulton Bank started receiving phishing e−mails over the weekend. Fulton said several of its customers have fallen for the scam. Fulton Bank officials said the bogus Website has now been taken offline, and that it originated somewhere in southeast Asia.
   Source: http://www.thewgalchannel.com/8onyourside/4685849/detail.htm l

6. *July 05, Associated Press* — **Three suspected in identity theft scam involving AOL subscribers.** Three people are facing identity theft charges for allegedly duping America Online (AOL) subscribers into divulging financial information then using it to go on a spending spree, police said Tuesday, July 5. Investigators arrested Jeffrey Brett Goodin of Azusa, CA, Mila Stroschein, and Christina Beeson, both of Covina, CA, after tracing a string of hotel room bookings, Ontario, CA, police Detective David McBride said. Authorities said Goodin, known as "The Hacker," is suspected of flooding America Online subscribers with e−mails asking them to update their personal billing information, including credit card number, address, Social Security and driver's license numbers, police said. Goodin used his computer to get e−mail addresses by accessing AOL's member directory, which is open to all subscribers, McBride said. Investigators allege Goodin, Stroschein and Beeson would use the financial information to book hotel rooms, make online purchases and withdraw cash from bank accounts. Investigators found personal identity data for people in Virginia and Georgia, among other states. Detectives were still tallying how much money had been stolen, McBride said.
   Source: http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/12060097.htm

[Return to top]

Transportation and Border Security Sector

7.

July 06, Associated Press — **Task force to investigate security at Sky Harbor after breach.** Despite a recent breach, officials at Sky Harbor International Airport in Phoenix, AZ, remain adamant that security at one of the nation's busiest airports is more than adequate. Still, a security task force is conducting a comprehensive review of the perimeter at Sky Harbor after a man driving a stolen truck was able to crash through a wrought−iron fence last week and drive onto the taxiway. The airport has shored up the damaged fence area with 18−inch high concrete barriers and is considering installing similar deterrents in other potentially vulnerable locations, including the employee parking lots. The task force is expected to recommend changes in addition to the enhancements already in place. Task force members include airline employees, airport personnel and representatives from such agencies as the Federal Bureau of Investigation and the Transportation Security Administration.
Source: http://www.usatoday.com/travel/news/2005−07−06−sky−harbor_x. htm

8. *July 06, Agence France−Presse* — **Lufthansa mulls digital fingerprinting at check in.** German airline Lufthansa said Wednesday, July 6, it hopes to introduce digital finger printing as early as next year and so−called "smart cards" to help speed up check−in procedures. Boarding passes are to be personalized with the passenger's thumbprint "if possible as early as next year," company spokesperson Thomas Jachnow said. The launch date could come before biometric finger printing is officially introduced in German passports and identity cards. Under the system, passengers submit a thumbprint at the check−in counter that is then checked at the boarding gate. The aim of the system is to prevent people who are not on the passenger list from boarding a plane. Frequent flyers could even be given smart cards that contain their digital fingerprint and other personal data. Asked about possible abuse of the data, Jachnow insisted that all personal information would be encoded, rendering it useless for outside parties.
Source: http://www.usatoday.com/travel/news/2005−07−06−lufthansa−fin gerpring_x.htm

9. *July 06, USA TODAY* — **Coast Guard plagued by breakdowns.** The Coast Guard's ships, planes and helicopters are breaking down at record rates, which may threaten the service's ability to carry out its post−9/11 mission of protecting ports and waterways against terrorism. Key members of Congress, maritime security experts and a former top Homeland Security Department official say that the fleet is failing and that plans to replace the Coast Guard's 88 aging cutters and 186 aircraft over the next 20 years should be accelerated. Former Coast Guard commandant and Homeland Security deputy secretary James Loy says "the stakes are simply too high in the post−9/11 environment" to continue to allow the Coast Guard's aging equipment to continue to deteriorate. Some ships are more than 50 years old, well beyond the recommended age for replacement. The Coast Guard was moved into the Department of Homeland Security in 2003 and given primary responsibility for maritime security in addition to its regular duties. The added responsibilities include patrolling the nation's 361 ports and 95,000 miles of coastline, boarding and inspecting tens of thousands of cargo ships and recreational boats, and reviewing security at the nation's commercial ports.
Source: http://www.usatoday.com/news/nation/2005−07−05−coast−guard_x .htm

10. *July 06, Associated Press* — **Rapid transit strike averted in California.** A Bay Area Rapid Transit (BART) walkout was averted early Wednesday, July 6, when unionized workers reached a deal with management less than two hours before the trains that carry more than 300,000 riders each day were threatened to be shut down. The agreement was announced by BART spokesperson Linton Johnson, just before 3 a.m. (PDT), ending more than four days of

round−the−clock negotiations that would have led to gridlocked freeways, overcrowded buses and ferries and a messy commute. BART management had said the major sticking point was finding a compromise that would help the agency deal with a projected $100 million, four−year deficit while not further burdening riders, who have already been hit with fare increases and parking charges. San Francisco Bay area transportation officials had urged commuters on Tuesday, July 5, to consider forming car pools, riding ferries, working from home and even taking vacations to keep the freeways moving if there was a strike. The last BART strike was in 1997 and lasted six days.
Source: http://www.usatoday.com/news/nation/2005−07−06−bart−nostrike_x.htm

11. *July 06, Associated Press* — **Little progress made on airplane tank flammability.** Nearly nine years after a fuel tank explosion caused the fatal crash of TWA Flight 800, safety officials say little has been done to reduce the flammability of vapors in aircraft fuel tanks. The Federal Aviation Administration (FAA) announced in February 2004 that it found a filtering system to make fuel vapors less likely to ignite. The agency said that it would propose in the fall of 2004 a regulation requiring that such systems be installed on large aircraft. National Transportation Safety Board executive director Dan Campbell said that little has been done to reduce the flammability of fuel vapors. Campbell acknowledged that the FAA has reduced sources of flame and sparks that can cause fuel vapors to explode. TWA Flight 800 crashed off the coast of Long Island, N.Y., on July 17, 1996, killing all 230 people aboard. In the past 15 years, there have been three fuel tank explosions, including the TWA accident, resulting in 346 deaths.
Source: http://www.macon.com/mld/macon/news/politics/12066873.htm

12. *July 06, Department of Transportation* — **University of South Florida receives grant for transportation education and research.** The Department of Transportation's (DOT) Research and Innovative Technology Administration (RITA) announced on Tuesday, July 5, that just over $1 million in grant money was awarded to the University of South Florida’s National Center for Transit Research, a DOT−funded University Transportation Center (UTC), to support the full range of the Center,s education and research programs. At the University of South Florida’s National Center for Transit Research, the principal focus is public transportation. Public transportation, broadly defined as alternatives to the single− occupant vehicle, includes modes such as carpool and vanpool, paratransit, bus, and guideway transit technologies. In addition, research activities focus on the interface of public transit with other transportation modes as well as the integration of public transit considerations within transportation and land use planning tools and procedures. The UTC program is administered by RITA and grant recipients are required to provide matching funds.
More information about the National Center for Transit Research can be found at http://www.nctr.usf.edu.
More information on UTC grants can be found at http://www.rita.dot.gov
Source: http://www.dot.gov/affairs/rita0505.htm

13. *July 05, Department of Transportation* — **University of Minnesota receives grant for transportation education and research.** The Department of Transportation’s (DOT) Research and Innovative Technology Administration (RITA) announced on Tuesday, July 5, that $3.1 million in grant money was awarded to the University of Minnesota's Intelligent Transportation Systems Institute, a DOT−funded University Transportation Center (UTC), to support the full range of the Institute,s education and research programs. The University of Minnesota’s

Intelligent Transportation Systems Institute is focused on enhancing the safety and mobility of road and transit−based transportation through “human−centered technology.” In addition, the Institute addresses issues related to transportation in a northern climate, investigates technologies for improving the safety of travel in rural environments, and considers social and economic policy issues related to the deployment of the core ITS technologies. The UTC program is administered by RITA and grant recipients are required to provide matching funds. More information about the Intelligent Transportation Systems Institute can be found at http://www.its.umn.edu.
More information on UTC grants can be found at http://www.rita.dot.gov
Source: http://www.dot.gov/affairs/rita0405.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *July 06, Agricultural Research Service* — **New fruit quarantine treatment.** A new technology called the Controlled Atmosphere/Temperature Treatment System (CATTS) may be coming to a packinghouse or plant quarantine facility near you. Developed by Agricultural Research Service (ARS) scientists, CATTS is a pesticide−free technology that kills codling moths, oriental fruit moths, and certain other insects with a lethal combination of rising temperatures and mixtures of low oxygen and high carbon dioxide. ARS entomologist Lisa Neven envisions using the technology as a post harvest treatment for apples, peaches, pears, cherries, and nectarines destined for export to foreign markets. Methyl bromide fumigation is a chief means of disinfesting such fruit, but the chemical is expensive, costing around $10 a pound, and its use is heavily regulated due to environmental safety and other concerns. In tests, CATTS killed 100 percent of codling moth larvae infesting apples, sweet cherries, peaches, and nectarines without significantly affecting the fruits' appearance, texture, taste and aroma, reports Neven. Oriental fruit moth tests are also promising, adds Neven. Ensuring pest−free fruit is vital to international trade. Otherwise, an importing country where a particular pest doesn't already occur may reject a fruit shipment or declare an all−out ban on further shipments.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Food Sector

15. *July 05, Virginian−Pilot* — **In Australia, salmonella strikes American travelers.** An educational trip to Australia took an ugly turn in recent days when more than a dozen children and adults fell ill with salmonella poisoning and had to be hospitalized. Of the 40 children and four adults from Virginia and North Carolina on the trip, 14 students and two leaders were treated at hospitals in Queensland, Australia, a spokesperson for People to People Student

Ambassador Programs said Tuesday, July 5. In all, 27 members of the group had symptoms of food poisoning. Health officials in Australia think members of the group ate contaminated food. The source of the outbreak is still under investigation. The first child fell ill Thursday, June 30, with what Australian health officials have confirmed is a type of salmonella. During a three− to four−day period more from the group became sick.
Source: http://home.hamptonroads.com/stories/story.cfm?story=88769&r an=10731

16. *July 05, Canadian Food Inspection Agency* — **Canada to implement monetary penalties for violations of mad cow safeguards.** The Canadian Food Inspection Agency (CFIA) announced Tuesday, July 5, that it will implement new monetary penalties to reinforce its system of safeguards to prevent the spread of mad cow disease, or bovine spongiform encephalopathy (BSE). Through amendments to the Agriculture and Agri−Food Administrative Monetary Penalties (AMPs) Regulations pursuant to the AMPS ACT, CFIA inspectors will be authorized to impose monetary penalties on operations which violate elements of Canada's system of BSE safeguards. With these changes, monetary penalties could be imposed for violations of two key safeguards: the BSE feed ban and requirements for the removal of specified risk material (SRM) from food products for humans. This will complement the monetary penalties that are already in place for failure to report suspected and actual cases of BSE. To date, enforcement tools available to the CFIA have been limited to warnings, seizure of products suspected of or known to be out of compliance, suspension or cancellation of permits, and prosecutions.
Regulatory Changes: http://canadagazette.gc.ca
Source: http://www.inspection.gc.ca/english/corpaffr/newcom/2005/200 50705be.shtml

17. *July 05, Daily Republic (CA)* — **Beef product seized over mad cow fear.** Federal officials seized beef consommé from a Fairfield, CA, grocery store earlier this spring, fearing the banned, Japanese−made food product might spread mad cow disease in the U.S. The consommé was accidentally allowed into the U.S. because the original label written in Japanese had been covered up by an English version that failed to list beef as an ingredient, according to a Solano County memo. Consommé is a clear, broth−like soup that uses meat and meat extracts for flavor. Japan is one of several foreign countries prohibited from exporting beef products to the U.S. Smuggling interdiction officials with the U.S. Department of Agriculture first found the banned consommé in Hawaii and worked with the importing company to find out where it had been shipped from there. They traced some of it to a small Fairfield market.
Source: http://www.dailyrepublic.com/articles/2005/07/06/business_to p_stories/biz01.txt

[Return to top]

Water Sector

18. *July 06, Trentonian (NJ)* — **Chlorination byproduct found in water supply.** Officials at the Trenton, NJ, Water Works announced Tuesday, July 5, that they have detected elevated levels of total trihalomethanes (THM) and haloacetic acids (HAA5) in the city's water supplies. THM are a group of four chemicals that form along with other byproducts when chlorine or other disinfectants used to control microbal contaminants in drinking water react with naturally occurring organic and inorganic matter in the water drawn for the city's supplies, according to the U.S. Environmental Protection Agency. HAA5 are also a group of chemicals that form when water treated with chlorine or other disinfectants react with germs or bacteria in the

water. Water works officials said there is not an immediate risk involved with the elevated levels and most residents do not have to drink bottled water.
Source: http://www.zwire.com/site/news.cfm?newsid=14810434&BRD=1697&PAG=461&dept_id=44551&rfi=6

[Return to top]

Public Health Sector

19. *July 06, Bloomberg* — **Indonesia struggles to halt polio as cases increase.** Indonesia's government is extending a vaccination campaign against polio as it struggles to contain the first outbreak of the disease in the country in a decade because some parents are refusing to let their children take the vaccine. The government is extending by three days the second round of a vaccination campaign that was supposed to end July 5, after it reached only four−fifths of the targeted children, Yusharmen, head of the immunization division at the Health Ministry, said. Polio, which has infected 111 children under five years since April, has spread outside the main island of Java. Health authorities provided 5.4 million children with the oral vaccine through July 4, 18 percent fewer than the 6.55 million children vaccinated in the first round in May, Yusharmen said. "There is growing resentment among the people because of wrong perception that they can get sick from the vaccine," Yusharmen said in an interview on Tuesday, July 5. This resentment magnified after five babies got sick after they received the vaccine, although investigations revealed that the babies died either from dengue or respiratory diseases. The next large−scale vaccinations will be held in August and September, World Health Organization said.
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=aS1Xtw93 3Uqk

20. *July 06, SciDev.Net* — **Africa to create center to fight infectious disease.** African nations have agreed to create a joint center in Cairo, Egypt, to fight infectious diseases afflicting the continent. Health ministers approved the plan at a conference held in Cairo on June 28−29. The African Union also backed the plan at meetings held this week in Libya. Ahmed Soliman Marai, an advisor to Egypt's health minister, stated that the center would help monitor and control infectious diseases by acting as a communications hub for information from health agencies across Africa, whose activities it would help coordinate. He added that the center will encourage and support research into drugs and vaccines against diseases endemic in Africa such as HIV/AIDS, malaria, tuberculosis, leishmaniasis, filariasis, and bilharzia. The center is also intended to promote affordable access to medicines, devise action plans in response to health threats, and provide training for health workers. The conference of health ministers set up a technical committee to draw up plans for funding the center and details of how it will work in coordination with existing African and international bodies. The committee, chaired by Egypt, comprises Algeria, Nigeria, Cameroon, Ethiopia and Uganda, South Africa, and a representative of the African Union.
Source: http://www.scidev.net/news/index.cfm?fuseaction=readnews&itemid=2205&language=1

21. *July 05, Associated Press* — **Cambodia suffering flu outbreak.** A 20−year−old man has become the latest fatality in a flu outbreak in Cambodia, where hospitals are crowded with children with respiratory infections and two infants have died in recent weeks, Health Minister

Nuth Sokhom said Tuesday, July 5. Thirteen other people from the orphanage were hospitalized with flu−like symptoms on Tuesday after eating chicken, he added. Megge Miller, a World Heath Organization (WHO) epidemiologist in Cambodia, said last week that some other sick children had tested positive for the influenza B virus, a common strain that can cause death, but does not have as high a fatality rate as the bird flu. Miller said she was waiting for laboratory test results for the current cases, expected Wednesday. The outbreak of influenza B has caused an unprecedented increase in the number of children sick with the virus at Cambodian hospitals and claimed the lives of two infant boys, nine and 14 months old, in recent weeks. More than 1,000 children have been hospitalized with what Sokhom described as a seasonal illness. The flu outbreak has strained impoverished Cambodia's grossly inadequate health care system, forcing at least one hospital to put three or four children to a bed.
Source: http://news.yahoo.com/news?tmpl=story&u=/ap/20050705/ap_on_he_me/cambodia_human_flu_1

22. *July 05, Agence France Presse* — **Turkish village quarantined after anthrax outbreak.** Turkish authorities quarantined a village in the southeast of the country after eight villagers were diagnosed with anthrax. Anthrax occurs when animals eat contaminated vegetation, absorbing bacterial spores that can live for decades. The outbreak was discovered when one of those taken ill, from the village of Cukurca, was taken to hospital in Bingol province. Health authorities identified seven other infected people in a subsequent check in the village. Two of those, a brother and a sister aged 10 and nine respectively, were in a life−threatening situation, the doctor treating them told the Anatolia news agency on Tuesday, July 5. Officials immediately imposed a ban on animals leaving or entering the village and began to destroy all the meat found in households, the report said. There are occasional anthrax cases in Turkey, especially in central and eastern parts, although authorities say the disease is on the wane and under control.
Source: http://news.yahoo.com/s/afp/20050705/hl_afp/turkeyanthrax_050705170120;_ylt=AqkiCpn9AVpGC6abVhm3f5OJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

23. *July 05, Xinhua News (China)* — **Six Asian countries join hands in combating communicable diseases.** Six countries in the Greater Mekong Subregion (GMS) −− China, Vietnam, Laos, Myanmar, Thailand and Cambodia −− on Tuesday, July 5, pledged to work together to prevent and control diseases that threaten either men or animals. According to a memorandum of understanding signed Tuesday in Kunming, capital of southwest China's Yunnan Province, the six countries will join together in combating such diseases as malaria, AIDS, avian flu, and foot−and−mouth disease. According to the document, the six countries will formulate policies and regulations on cross−border transfer of animals, raise immunity of animals from diseases, create an early−warning system for animal−related diseases, improve construction of veterinarian network, monitoring and diagnosis capability, and strive to build an emergency aid mechanism against an outbreak of cross−border animal diseases. Jin Liqun, deputy president of the Asian Development Bank (ADB), GMS members are responding to the threats of infectious diseases, including avian flu and HIV/AIDS, through a regional program of communicable disease control. In implementing this program, the poor and vulnerable groups in border areas are given special focus, said the deputy president.
Source: http://news.xinhuanet.com/english/2005−07/05/content_3179262 .htm

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24. *July 06, Bennington Banner (VT)* — **Emergency response gets tested in Vermont.** The town of Bennington, VT, will host the region's first full−scale emergency drill Thursday, July 7, featuring a mock car chase between police and a "suspected terrorist" who wants to steal a plane, cram it with explosives and fly it into the Vermont Yankee Nuclear Power Plant in Vernon. The drill will feature gunshots, hostages, a fire, and, of course, a getaway plane. The drill is being held so local and federal inspectors can review the response of police, fire, and rescue personnel in the event of an actual terrorist threat. It will also judge how well the departments work together. The Local Emergency Planning Committee is working with support of the Bennington County Regional Commission to hold the drill to fulfill a requirement of Homeland Security guidelines. The drills, which take months to plan, will likely become annual or semi−annual. Upwards of 40 to 50 emergency responders, possibly including mutual aid personnel, could participate depending on the number of people available at the time of the drill.
Source: http://www.benningtonbanner.com/Stories/0,1413,104~8676~2952 893,00.html

25. *July 06, Brattleboro Reformer (VT)* — **Evacuation plans may not work for childcare centers.** There are approximately 677 children enrolled in licensed childcare centers and homes throughout the 10−mile radius around the Vermont Yankee nuclear power plant in Vernon. That figure swells to 877 when older children arrive for after−school care. The area surrounding Vermont Yankee is known as the emergency planning zone and state and local officials are responsible for maintaining a detailed plan in the event of a radiological release from the reactor. Childcare centers and homes are expected to have emergency response plans, but there has been concern that the plans are not workable. One of the challenges facing providers is that there is no centralized transportation system; children are usually dropped off by their parents. In the event of a mandated evacuation, Brattleboro Town Manager Jerry Remillard said the town would arrange to transport any child in care that needs it, using the schools' bus contractor. According to Duncan Higgins of Vermont Emergency Management, providers are expected to have enough car seats on hand to safely transport the children, as well as any equipment necessary for children with special needs. Such a requirement, however, is not part of the state's licensing regulations for childcare centers and homes.
Source: http://www.reformer.com/Stories/0,1413,102~8860~2952965,00.h tml

26. *July 06, Chicago Sun−Times* — **Computer taken off−line twice at 911 center.** A slow−running computer server at a 911 emergency center in Chicago, IL, was taken off−line twice −− for a total of nearly three hours −− Monday, July 4, and Tuesday, forcing call takers to switch to a manual backup system on one of the busiest days of the year. Testing is still being conducted to determine what caused the server to run slow. The computer trouble started

shortly before 11:30 p.m. Monday as crowds were heading home from the Taste of Chicago finale, and fireworks celebrations were winding down. According to Monique Bond, a spokesperson for the city's Office of Emergency Management and Communications, 911 call takers began to notice that "transactions were running slow," meaning that forms they are required to fill out about every call were "slow to transition from one form to another." Instead of taking a chance that the problem would get worse, the slow−running computer server was "taken off−line" from 11:29 p.m. until 12:31 a.m. That allowed engineers who were "on standby" in the event of just such a problem to conduct a series of diagnostic tests. The server was back online after the one−hour, two−minute test.
Source: http://www.suntimes.com/output/news/cst−nws−phone06.html

[Return to top]

Information Technology and Telecommunications Sector

27. *July 05, Secunia* — **EasyPHPCalendar "serverPath" file inclusion vulnerability.** A vulnerability has been reported in EasyPHPCalendar which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "serverPath" parameter isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. The vulnerability has been reported in version 6.1.5 and prior. Other versions may also be affected.
Source: http://secunia.com/advisories/15893/

28. *July 04, The Register* — **Symbian Trojan drains the life from phones.** Virus writers have created a new Symbian Trojan called Doomboot−A that loads an earlier mobile virus (Commwarrior−B) onto vulnerable smartphones. Doomboot−A also preventing infected phones from booting up properly. "Doomboot−A causes the phone not to boot anymore and Commwarrior causes so much Bluetooth traffic that the phone will run out of battery in less than one hour. Thus the user who gets his phone infected with Doomboot−A has less than one hour to figure out what is happening and disinfect his phone, or he will lose all data," writes Jarno Niemela, a researcher at Finnish anti−virus firm F−Secure. "The Doomboot−A installation does not give any obvious clues that something is wrong, and Commwarrior−B does not have icon and is not visible in the process list. So the installation of Doomboot−A looks very much like failed installation of pirate copied game, and [a] user has hard time noticing that something bad is happening," he added. Doomboot−A, like most Symbian Trojans, poses as a pirate copy of a Symbian game (in this case Doom 2). Users who avoid pirated games or applications should be safe from infection.
Source: http://www.theregister.co.uk/2005/07/04/symbian_trojan_doomb oot/

29. *June 28, SecurityFocus* — **Sun Solaris Runtime linker LD_AUDIT privilege escalation vulnerability.** Runtime linkers in most operating systems are designed to ignore LD_* environment variables when executing setuid or setgid binaries. The manual page describing ld.so for Sun Solaris also states that certain precautions are taken when setuid or setgid binaries are executed. Reportedly these precautions are not properly followed when LD_AUDIT is utilized. This vulnerability allows local attackers to gain superuser privileges on affected computers.

Sun has released Interim Diagnostic Relief fixes to address this issue:
http://sunsolve.sun.com/tpatches
Source: http://www.securityfocus.com/bid/14074/discuss

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 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 (−−−), 139 (netbios−ssn), 135 (epmap), 8956 (−−−), 6346 (gnutella−svc), 32775 (sometimes−rpc13), 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

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[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.

DHS/IAIP Disclaimer