Department of Homeland Security Daily Open Source Infrastructure Report for 12 June 2008

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- The Chicago Tribune reports that debris as small as a pebble on a runway poses a greater safety hazard on runways than plane collisions. The airline industry estimates that runway debris causes at least $1 billion in damage to commercial aircraft and it affects planes in about 70,000 incidents each year. (See item **17**)
- WOWK 13 in Charleston reports that the West Virginia Department of Military Affairs and Public Safety, Homeland Security, and dozens of emergency offices across West Virginia will practice an emergency drill on how to deal with millions of people evacuated from the Washington - Baltimore region. (See item **29**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

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

1. *June 11, Bloomberg* – (International) **World faces 'oil crisis;' IEA ready to tap reserves.** The world faces an "oil crisis," and the International Energy Agency (IEA) stands ready to release emergency stockpiles even as the biggest consumers discuss measures to contain spiraling demand, the agency's chief said. "Any major oil-plant accident can cause a supply disruption," the executive director said. "We at the IEA are monitoring the oil market and preparing ourselves to call for the release of strategic petroleum reserves at any time in the event of a major disruption." "We can call it an 'oil crisis' given the current price, and that it continues to climb even after global efforts

to cut consumption," he said. "We see a critical, structural issue in the global oil market, where supply growth isn't catching up with demand." Unlike the oil crisis in the 1970s, which was driven by supply restraints from the Middle East, the current situation is fueled by soaring demand, the IEA chief said. Speculative investment in commodities is also a driving force behind record prices, he said.
Source: http://www.bloomberg.com/apps/news?pid=20601072&sid=a0SE24WXEk5U&refer=energy

2. *June 11, Reuters* – (International) **Nigeria oil union see Chevron talks averting strike.** Nigeria's white-collar oil workers' union said on Wednesday it was optimistic that negotiations to avert a strike at the local unit of Chevron would be productive. The Chevron branch of the PENGASSAN union had threatened to begin a potentially crippling strike last week to press for the transfer of the expatriate managing director out of Nigeria, but the national executive intervened to halt a walkout. "As it is now, there won't be any strike, we are monitoring the talks and are ready to intervene at anytime if the talks stall," said PENGASSAN's deputy national secretary. "We have not given the two parties any time-frame to reach a deal, the issues could be resolved today or it may take them a week, but we are optimistic," he said.
Source: http://www.reuters.com/article/marketsNews/idUSL1118595820080611

3. *June 11, Marshalltown Times-Republican* – (Iowa) **Power plant shut down to avoid flood damage.** Alliant Energy's Sutherland Generating Station was shut down Monday to protect its operations from flood damage, but no power outage is expected as a result. Sandbags were stacked around a substation and the plant's control building. Approximately 50 megawatts of electricity generation from Units 1 and 2 were powered down during the day, said an Alliant spokesperson. Unit 3 was already offline for a construction project. Electricity is still being supplied to the regional grid from other power generating sources, he said, and no power outage is expected locally unless as a result of future storms. "Any impact of the Sand Lake levee wouldn't have further damage [to the plant]," he said. "Our concern is the river level." Staff are visiting the plant to monitor its status, and it will not reopen until flooding concerns subside, he said.
Source: http://www.timesrepublican.com/page/content.detail/id/507189.html?nav=5005

4. *June 11, San Francisco Chronicle* – (California) **Wind-whipped blaze hits 33 homes in Stockton.** Firefighters throughout the Bay Area were kept busy fighting grass and brush fires. Workers at the Aidlin Geothermal power plant east of Cloverdale kept a worried eye on a 700-acre fire that began around 10 a.m. chewing through wildland brush and trees. Six air tankers and five helicopters were dumping retardant and water from above while 150 firefighters attacked on the ground. "We don't have any evacuations, but we're hitting it hard to keep it away from the plant," said a spokesman for the state Department of Forestry and Fire Protection.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/06/11/BAV0116Q5A.DTL

5. *June 10, CBS 3 Philadelphia* – (Pennsylvania) **Truck explodes at PGW facility.**

Investigators are trying to determine why a truck carrying compressed natural gas exploded at the Philadelphia Gas Works facility in Port Richmond Monday. Authorities said the explosion happened at about 2 p.m. on the grounds of the facility. A second tank inside the vehicle did not explode. No injuries were reported. The Philadelphia Fire Marshall's Office has joined the investigation.
Source: http://cbs3.com/topstories/pgw.explosion.natural.2.743959.html

6. *June 9, KWTX 10 Waco* – (Texas) **FBI joins investigation after explosives recovered from car, local home.** The Federal Bureau of Investigation is joining the investigation after a weekend police chase that started in central Texas and ended south of Austin led to the discovery of weapons and explosives in the vehicle and home of a Morgan's Point man. The chase started around 1:45 a.m. Saturday when Morgan's Point police spotted a suspicious vehicle near fuel tanks at Morgan's Point Marina. The driver of the late model Mustang sped off as officers approached. Belton Police, State Troopers and Williamson County and Travis County deputies were all involved in the chase, which finally ended when the man crashed the car south of Austin. Police say he shot himself in the face as officers approached the wrecked car. Authorities said he is expected to survive. The Austin Bomb Squad was called to the scene after explosives, ammunition, and weapons were found in the vehicle and dismantled the devices. Fort Hood's Explosive Ordinance Detachment Team was dispatched to the man's residence about 6:15 a.m. Saturday. The U.S. Alcohol, Tobacco, and Firearms dispatched a field agent, a bomb tech, and a bomb-detecting dog to the scene. Authorities recovered what they said were materials for making pipe bombs. The FBI asked that the affidavit submitted for the search warrant and the search warrant be sealed.
Source: http://www.kwtx.com/home/headlines/19664369.html

7. *June 9, Grand Junction Sentinel* – (Colorado) **Gas site workers contain fire quickly.** A pit caught fire at a natural gas development site north of Parachute Monday morning, but workers on the scene were able to shut down the flow to the pit and the fire burned itself out, officials said. The fire occurred at an EnCana Oil & Gas site on EnCana's North Parachute Ranch. The fire occurred in a produced water flowback pit, said an EnCana spokesperson. When firefighters arrived, they learned that the workers had shut down operations at the scene and the fire eventually went out. The EnCana spokesperson said workers had evacuated others from the area and closed off access to safeguard the scene. No one was injured in the fire. Property damage was limited to scorched pipes leading to the evaporation pit. The cause of the fire remains under investigation, she said.
Source:
http://www.gjsentinel.com/hp/content/news/stories/2008/06/09/061008_1B_well_fire.html

[Return to top]

Chemical Industry Sector

8. *June 11, KRIV 26 Houston* – (Texas) **6 Injuries reported in Southeast Houston chemical plant fire.** At least six people have been injured Wednesday morning in a fire at a chemical plant for Goodyear in southeast Houston. No flames could be seen,

however it is reported the plant is leaking ammonia. The extent of the injuries involved is unknown, however one person has been listed in critical condition. No evacuations or threats to the community have been reported, but workers at a neighboring plant have been ordered to shelter in place.
Source:
http://www.myfoxhouston.com/myfox/pages/News/Detail?contentId=6744049&version=3&locale=EN-US&layoutCode=TSTY&pageId=3.2.1

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

9. *June 11, Des Moines Register* – (Iowa) **Flooding around the state.** In Palo, a small army of volunteers filled sandbags Tuesday as they braced for record flooding on the Cedar River that threatens to engulf about four-fifths of this Linn County town of 900. Levels are expected to exceed 1993 flooding. The Linn County sheriff said the Duane Arnold Nuclear Energy Center is not in danger of being flooded, and the plant has made preparations to ensure there will be sufficient workers to safely operate the facility.
Source:
http://www.desmoinesregister.com/apps/pbcs.dll/article?AID=/20080611/NEWS/806110373/-1/BUSINESS04

10. *June 10, Associated Press* – (Colorado) **Small amount of plutonium spills at NIST exposes 22 workers.** A vial with about a 1/4 gram of powder containing plutonium cracked and spilled radioactive particles in a lab, exposing 22 workers at the National Institute of Standards and Technology (NIST) to trace contamination. Two workers, who had worked directly with the radioactive material Monday, got rid of the contamination by washing their hands. NIST officials said most of the 20 other nearby workers had trace contamination on their shoes and clothing, which was washed off. Workers were using the plutonium containing powder for a project to improve radiation detectors for use by nuclear inspectors. The lab has been sealed off. A NIST spokesman on Tuesday said the incident has been reported to the U.S. Nuclear Regulatory Commission.
Source: http://www.krdo.com/Global/story.asp?S=8460705&nav=menu552_1

[Return to top]

Defense Industrial Base Sector

11. *June 11, Jane's* – (National) **Blue-force tracking evolves for the modern battlefield.** An automatically updating system that shows the location of all friendly forces removes any question over accuracy and, in theory, is always current. Positional data can be automatically filtered and aggregated by sub-unit and unit, so that as the information moves up the command chain, it is shown at a level appropriate to the viewer, and can also be expanded if required. As the data is available to all, in the same time frame, everyone is working to the common operating picture and misunderstandings should be reduced. However, a system that relies purely on terrestrial radio communications is

affected by range limitations and terrain interference, for when communications are interrupted data is no longer updated. The updating interval or the refresh rate is the planned delay in the system, and most systems rely either on a time or a distance-moved trigger. The parameters of these triggers can be varied, and may be changed according to the tactical situation. The latency of the system is the unplanned delay or the delay caused by the time it takes to transmit, manipulate, and retransmit the data. These blue-force tracking systems therefore do not provide a real-time image of the battlefield. While going a considerable way towards force deconfliction, they do not offer fail-safe combat identification. The reliance on global positioning system can be a disadvantage in the urban environment, where the system is less effective, particularly at the level of the individual soldier inside a building.
Source: http://www.janes.com/news/defence/land/idr/idr080611_2_n.shtml

[Return to top]

Banking and Finance Sector

12. *June 10, Columbia Tribune* – (Missouri) **Phishing scam targets Central Missouri bank.** Spammers are using Boone County National Bank’s logo in an e-mail message that asks recipients to click on a hyperlink and enter personal information. The message, which says “Notice” in the subject line, says that a statement is available for viewing and provides a link to access the statement. Although the bank’s name is spelled correctly in the logo, the message says, “Boone Country National Bank.”
Source: http://www.columbiatribune.com/2008/Jun/20080610Busi001.asp

[Return to top]

Transportation Sector

13. *June 11, USA Today* – (National) **FAA turns attention to medical flight crashes.** Federal aviation officials said Monday that they are concerned medical helicopter accidents may again be on the rise now that four fatal crashes have happened in less than six months. All four of the recent fatal crashes happened at night and in places where pilots had little or no visual reference on the ground, such as a forest or over water, according to the National Transportation Safety Board (NTSB) files. “We’re monitoring all these recent investigations with an eye towards whether they are related to previous recommendations we made,” said the deputy director of the NTSB’s aviation division. The NTSB said in 2006 that most crashes were preventable. It issued recommendations for better technology and new rules to force pilots to be more cautious, especially at night and in poor weather. The NTSB recommended that air-ambulance companies adopt new technology to warn pilots when they flew too close to the ground and to pay more attention to high-risk factors such as poor weather before departing. The NTSB also voted to encourage the Federal Aviation Administration (FAA) to approve the use of night-vision goggles. The new technology has proved difficult to put in place, according to FAA documents and a program director for LifeFlight of Maine. None of the pilots on the four recent fatal crashes at night was using night-vision goggles, according to the NTSB official.

Source: http://www.firerescue1.com/news/404328-FAA-turns-attention-to-medical-flight-crashes/

14. *June 10, Courier-Journal* – (Kentucky) **Two barges collide with sunken remains.** Two barges were damaged and started leaking Tuesday morning after they collided with two sunken barges still waiting to be raised from the Ohio River. About 4 a.m., the tow boat O.C. Clark was traveling up-river with 15 barges loaded with coal, said a lieutenant with the U.S. Coast Guard. The barges rubbed the side of the sunken barges, which sunk near the dock of the Belle of Louisville, Kentucky, after coming loose from another tow boat on Friday. The contact damaged two of the Clark barges, causing them to start taking on water, the official said. The barges made it to safety and have been patched, he said. No coal went into the river, and no one was hurt in the incident. Coast Guard and Army Corps of Engineers officials are awaiting a salvage plan on how to get the two sunken barges out of the river, which the lieutenant said is expected this morning from the Ingram Barge Co. Traffic along the river has been disrupted several times since the two barges, which were carrying powdered iron ore, sunk Friday.
Source: http://www.courier-journal.com/apps/pbcs.dll/article?AID=/20080610/NEWS01/806110735/1008

15. *June 10, CNN* – (National) **NTSB: Pilots' long hours leading to accidents.** Responding to recent accidents linked to pilot fatigue, federal safety officials hope reduce airline pilots' logging 14-hour days. The Federal Aviation Administration (FAA) currently allows pilots to log 14-hour workdays, which the National Transportation Safety Board (NTSB) says contributes to accidents. The NTSB concluded in a report out Tuesday that pilot fatigue was a probable cause in a runway landing accident during bad weather in Michigan last winter. The FAA currently allows a 14-hour workday with eight hours of logged airtime. "Fourteen hours is still a very long day," a NTSB board member said. Her conclusion is backed by 40 years of airline accident statistics compiled by the FAA and cited Tuesday at an NTSB hearing. "After a duty period of about 10 to 12 hours, the number of observed accidents increased exponentially," a NTSB staff member said. The NTSB report called for analysis of sleep quantity, sleep quality, performance, errors, and incidents traced to schedules that disrupt sleep patterns, perhaps while stretching workloads to the maximum allowed. After reviewing some possible remedies against fatigue in the cockpit, board members unanimously approved the proposal to the FAA, which would be responsible for developing guidance for the airlines to carry out.
Source: http://edition.cnn.com/2008/US/06/10/sleepy.pilots/

16. *June 10, Associated Press* – (National) **IG criticizes FAA's training of air controllers.** The government is hiring so many new air traffic controllers to replace departing veterans that it cannot efficiently train them, an inspector general reported Tuesday. The Transportation Department's inspector general said the Federal Aviation Administration (FAA) is so swamped with new hires that it has exceeded its own maximum trainee numbers at 22 percent of its 314 air control facilities. The FAA uses a database replete with erroneous information to manage the training program and has failed to implement remedial steps the agency itself promised in 2004, the IG report added. In a written

response, the FAA accepted most of the IG's recommendations. But the FAA rejected the idea of making public an accurate count each year of how many fully certified controllers and how many trainees work in each of its facilities. New hires off the street or emerging from the FAA academy and even veteran controllers transferring to a new facility all must undergo on-the-job training to qualify to work each radar position at their new workplace. This can take up to three years before they are fully certified to work all stations.
Source:
http://ap.google.com/article/ALeqM5gR4vVByQBFK39PU_3HbVj8jdxY4AD917H6PO3

17. *June 10, Chicago Tribune* – (National) **Airports attack threat from runway debris.** Debris as small as a pebble on a runway can be a potential hazard for planes, making the clearing of airfields both essential and a challenge. In aviation parlance, "FOD," or foreign object debris, can be sucked into jet engines or slice through the thin aluminum skins of aircraft, potentially setting off catastrophic fuel-tank explosions. In fact, to the astonishment of some aviation experts, recent studies suggest that debris poses a greater safety hazard on runways than plane collisions. The heightened concerns have spurred the Federal Aviation Administration to test high-tech ways to detect debris beginning this month at Chicago's airports. Putting radar surveillance technology and infrared cameras to a new use, a database has been created by scrutinizing every inch of runways, taxiways and ramp areas at an airport. Software-mapping systems memorize every runway light, every sign, every crack in the pavement. Anything that doesn't appear to belong on the airfield shows up on a screen that displays its exact location using global positioning system software. An airport worker is then dispatched to remove the debris. For years, airports relied on ground personnel and even pilots on takeoffs and landings to make visual inspections for debris. But it is akin to finding the needle in a haystack on runways that can stretch longer than 2 miles. The airline industry estimates that runway debris causes at least $1 billion in damage each year to commercial aircraft. Runway debris causes damage to planes in about 70,000 incidents each year at the 300 largest airports in the world, according to a study issued in March by the research firm Insight SRI. Airlines incur costs as high as $20 million annually from the problem at some airports, the study said. The debris can vary from ball bearings and eating utensils to mechanics' tools and fuel caps.
Source: http://www.chicagotribune.com/news/nationworld/chi-runway-debrisjun11,0,7048450.story

18. *June 10, KCAL 9 Los Angeles* – (California) **Southwest plane gets too close to runway at LAX.** A Southwest Airlines 737 jetliner got within 140 feet of a runway on which another aircraft was about to land at Los Angeles International Airport (LAX), instead of staying the required 205 feet away, authorities said Tuesday. The runway incursion, which was considered to be minor, occurred about 9 a.m., according to a Federal Aviation Administration spokesperson. He said the Boeing 737 was about 65 feet over a "hold line." The SkyWest Airlines turboprop landed safely after the pilot received instructions from a controller, the official said.
Source: http://cbs2.com/local/Southwest.Airlines.737.2.744911.html

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

19. *June 11, Billings Gazette* – (Montana) **Cattle industry losses could reach millions.** Montana's cattle industry will take at least a $6 million hit for losing its brucellosis-free status, said insiders, who called damage inevitable after a Paradise Valley heifer tested positive for the disease. Auction block prices are not likely to slip, but the cost of assuring the rest of the country that Montana's cattle are disease-free is expected to mushroom. For years, the state has gotten by with testing only a small percentage of its cattle for brucellosis. The number of cattle tested in Montana will increase more than tenfold. A brucellosis test costs $1.50 or less, but the real expense is in rounding up the cattle for testing, hiring a veterinarian to draw blood and keeping the cattle corralled until the results come back. The roundup and the testing are likely to cost $12 to $15 per animal. Corralled cattle also must be fed hay at a cost of $1 per day, per animal, and ranchers worry that the cattle will have to stay there at least a week while they wait for the results.
    Source: http://www.billingsgazette.net/articles/2008/06/11/news/state/21-industry.txt

20. *June 11, Northwest Arkansas Times* – (Arkansas) **Avian flu detected at county farm.** At least one sample from a breeder hen flock near West Fork has tested positive for the live virus of low pathogenic avian influenza, according to a memo released Tuesday by the Arkansas Livestock and Poultry Commission in Little Rock. U. S. Department of Agriculture officials notified the commission about the sample this week. Preliminary tests on the flock last week indicated the presence of antibodies for H7N3, which is a mild type of avian influenza, commonly referred to as 'bird flu,' that officials say is not a danger to humans. Upon the discovery, the 15,000 chickens owned by Tyson Foods Inc. were killed on June 3, and their carcasses have been buried on the farm. The discovery of this mild form of avian influenza poses no food safety or human health risk, according to a statement released by a Tyson Foods spokesman. He noted that additional testing of more than 50 area farms was initiated last week, and increased biosecurity, placing additional limits on access to poultry farms, has been implemented.
    Source: http://nwanews.com/nwat/News/66080/print/

21. *June 10, Reuters* – (National) **New food safety scare takes toll on consumers.** Outbreaks of food-borne illness are scaring people away from some foods and shaking their confidence in U.S. food safety procedures. Over the last few years, consumers have digested reports of tainted spinach, peanut butter, and pot pies. A new poll commissioned by Deloitte Consulting pointed to growing concerns about food safety. Out of 1,100 respondents, 76 percent were more concerned about the food they eat than five years ago, while 73 percent believed the number of food-related recalls have risen

in the past year. Fifty-seven percent of respondents stopped eating a particular food, temporarily or permanently, following a recall.
Source:
http://www.reuters.com/article/healthNews/idUSN1037615120080610?feedType=RSS&...

[Return to top]

Water Sector

22. *June 11, Associated Press* – (Wisconsin) **Private drinking water at risk because of flooding.** Flooding in Wisconsin is raising concerns about possible contamination of private wells. The Department of Natural Resources (DNR) is urging well owners in flooded areas to make sure their water is safe to drink. A DNR water specialist says bacterial, viral, parasitic, or chemical contamination carried in floodwater can seep into a well's casing and make drinking water unsafe. About 750,000 Wisconsin residents drink water from private wells.
Source: http://www.chicagotribune.com/news/chi-ap-wi-severeweather-wel,0,5481137.story

23. *June 10, Burlington Free Press* – (Vermont) **Douglas signs groundwater protection bill.** Vermont's governor signed a bill Monday that is expected to give the state and residents more say in large extractions of groundwater. The legislation declares Vermont's groundwater a public trust and sets up a permitting process for those who want to make large water withdrawals. It is meant to protect Vermont from water-shortage problems other states are seeing, but also to prevent problems Vermont has seen with wells going dry, streams losing flow, and neighbors having little control over projects that might affect them, said a representative of the Vermont Natural Resources Council, which supported the legislation. The law will require commercial enterprises that withdraw 20,000 gallons a day or more to file a report with the state starting September 1, 2009, and to obtain a permit for withdrawal of more than 57,000 gallons effective July 2010. Most farming operations will be exempt. That means the state should be able to better monitor how much water is being withdrawn and make sure it has no adverse impact on surrounding water supplies.
Source:
http://www.burlingtonfreepress.com/apps/pbcs.dll/article?AID=/20080610/NEWS02/806100306

[Return to top]

Public Health and Healthcare Sector

24. *June 11, Reuters* – (International) **Hong Kong begins mass bird cull as H5N1 spreads.** Hong Kong, hoping to stop the spread of the feared H5N1 bird flu virus among the city's many markets, will begin culling live poultry across the city, government officials said on Wednesday. Hong Kong last week found H5N1 at a poultry stall in one of the many so-called wet markets and ordered the culling of 2,700 birds. But the virus had

since spread among the island's poultry population and mass cullings were now necessary as a precaution, they told reporters. Officials did not say if any people had been infected.
Source: http://www.reuters.com/article/asiaCrisis/idUSHKU0001014

25. *June 11, Daily Utah Chronicle* – (Utah) **U hospital billing records missing.** Billing records for about 2.2 million U Hospital and Clinics patients and guarantors were stolen from a company working for the U on June 2 in Salt Lake City. A metal box containing backup tapes was stolen from a car that belongs to an employee of an independent moving company Perpetual Storage Inc. The encrypted tapes contain information on patients who were seen by a provider connected with the hospitals within the past 16 years. The U Hospital and Clinics hired the company to move its records to an off-site vault to secure them from disasters such as fire or earthquakes. According to company protocol, the employee was supposed to use a company van to move the records and take them directly to the vault. Instead, the employee used his own car to pick up the records from the hospital and drove home. When the police were told what was in the box, they contacted the FBI because the information could be used to commit identity theft, especially because it contained 1.3 million Social Security numbers.
Source:
http://media.www.dailyutahchronicle.com/media/storage/paper244/news/2008/06/11/News/U.Hospital.Billing.Records.Missing-3380644.shtml

26. *June 10, Cortex Journal* – (Colorado) **Health officials watch virus.** Public-health officials in Montezuma County and all over Colorado are urging residents to take precautions to escape hantavirus this year. So far, four cases of hantavirus-pulmonary syndrome have been reported in 2008, with one resulting in a fatality. The most recent cases were confirmed in late May within Delta and Dolores counties. "It's everywhere. It's in the eastern part of Colorado and moving its way west," said Montezuma County's Health Department director. Two previous cases of hantavirus were reported in Kiowa County in February and another Fremont County in early May. The patient in Kiowa County died. Hantavirus is a respiratory disease carried by deer mice, which are common to rural areas throughout the state. Deer mice are brown on top and white underneath, with large ears relative to their head size. The virus can infect humans who inhale dirt and dust contaminated with deer mice urine and feces when working in rodent-infested structures.
Source: http://www.cortezjournal.com/asp-bin/article_generation.asp?article_type=news&article_path=/news/08/news080610_3.htm

27. *June 10, KTIV 4 Sioux City* – (Iowa) **Floodwaters can be 'breeding ground' for virus-carrying mosquitoes.** The recent rain in Siouxland, Iowa, has left standing water that is prime breeding grounds for mosquitoes that could be carrying the West Nile Virus. A Siouxland District Health Department official, said, "Usually, the West Nile virus will start about this time of the year in the United States. But, around Iowa, it will generally peak around August, but it doesn't mean you can't get it now. Recently, this year, we have had a lot of water and there is a lot of breeding ground all around us." There are

many areas like this around Siouxland due to flood-like conditions. There were three fatalities from the West Nile Virus in Iowa last year.
Source: http://www.ktiv.com/News/index.php?ID=26160

[Return to top]

Government Facilities Sector

Nothing to report

[Return to top]

Emergency Services Sector

28. *June 11, Denver Post* – (Colorado) **Hospitals hold disaster drill.** Eight Denver hospitals held drills Tuesday to test their abilities to respond to a disaster that would injure thousands of people. The mock exercise — a “dirty bomb” explosion at a Pepsi Center packed with 20,000 people — was one of the largest-ever cooperative drills for the city’s hospitals, organizers said. It comes just two months before the Democratic National Convention, when the city will host thousands of people from around the world. About 140 volunteers participated in the citywide drill, many of them acting as victims. Though the hospitals knew there would be a drill, the details became known only as the scenario unfolded. Each hospital will receive an evaluation for Tuesday’s exercise.
Source: http://origin.denverpost.com/politics/ci_9544375

29. *June 10, WOWK 13 Charleston* – (West Virginia) **Major statewide emergency drill planned.** In a drill sponsored by the West Virginia Department of Military Affairs and Public Safety, Homeland Security and dozens of emergency offices across the state, West Virginia emergency workers will practice on how to deal with major evacuations from the Washington - Baltimore region. Crews will practice getting ready for millions of people evacuating the Washington - Baltimore metro following a dirty bomb explosion. More than 20 counties are involved in the drill at some level. The purpose is to evaluate equipment, communications, response and personnel at all levels of response. Authorities hope to solve any problems that exist during this drill when lives are not at stake. The drill starts next Tuesday at 9 a.m.
Source: http://wowktv.com/story.cfm?func=viewstory&storyid=39825

[Return to top]

Information Technology

30. *June 11, Associated Press* – (National) **Security hole exposes utilities to Internet attack.** Attackers could gain control of water treatment plants, natural gas pipelines and other critical utilities because of a vulnerability in the software that runs some of those facilities, experts with Boston-based Core Security Technologies reported Wednesday. Citect Pty. Ltd., which makes the program called CitectSCADA, patched the hole last

week, five months after Core Security first notified Citect of the problem.But the vulnerability could have counterparts in other so-called supervisory control and data acquisition, or SCADA, systems. And it is not clear whether all Citect clients have installed the patch. SCADA systems remotely manage computers that control machinery, including water supply valves, industrial baking equipment and security systems at nuclear power plants.Customers that use CitectSCADA include natural gas pipelines in Chile, major copper and diamond mines in Australia and Botswana, a large pharmaceutical plant in Germany and water treatment plants in Louisiana and North Carolina. For an attack involving the vulnerability that Core Security revealed Wednesday to occur, the target network would have to be connected to the Internet. That goes against industry policy but does happen when companies have lax security measures, such as connecting control systems' computers and computers with Internet access to the same routers. A rogue employee could also access the system internally. Source: http://ap.google.com/article/ALeqM5g2Z6WkZ3cMTEiJJFaV9YDX5Eg4xAD917P72G2

31. *June 11, TechNews World* – (International) **The Storm Worm's elaborate con game.** Security researchers at Cisco's IronPort say they have pieced together the complex con operation behind the Storm Worm, a persistent Web threat. The botnet's purpose, they say, was essentially to act as a virtual dealer of prescription – and often bogus – medication, sometimes enlisting work-from-home employees who thought they were doing legitimate tasks. Despite their discovery of a direct link to the funding sources behind the infamous Storm Virus, IronPort Systems researchers are doubtful law enforcement will ever catch the perpetrators. Still, improving technologies may help to block its continuing spread. IronPort announced its discovery of an online criminal ecosystem comprised of illegal pharmaceutical supply chain businesses that recruit botnets to send spam promoting their Web sites. By converting spam into high-value pharmaceutical purchases, these supply chain enterprises allow the monetization of spamming botnets, providing an enormous profit motivation for botnet attacks and continuous innovation. IronPort's study points to these fake drug traffickers as large sources of funding for Storm virus technology. Among the more insidious related criminal activities involves the enlistment of workers to collect and deliver funds from phishing and fraud schemes that have been initiated through the Storm virus. Source: http://www.technewsworld.com/story/The-Storm-Worms-Elaborate-Con-Game-63357.html?welcome=1213186145

32. *June 11, TradeArabia News Service* – (International) **IronPort detects new trojan horse.** IronPort Systems, a leading e-mail and web security products provider, has detected a new malicious Trojan Horse program. IronPort's S-Series Web Reputation Filters were able to capture, identify, report and respond against the new internet threat, which uses a fake anti-spyware website, http://antispyware911.com, to lure internet users to download a phony scanner containing the Trojan, the company said. It said the program has not been identified by other leading web security systems. The bogus website claims to be a free fix for a spyware; users who accept the offer unsuspectingly download the malicious Trojan. Unlike infectious malicious programs such as viruses,

such Trojan horse codes do not propagate by self-replication but instead rely on the exploitation of an end-user. IronPort's latest discovery reflects the prevalence of malevolent social engineering throughout the internet, where trickery is used to gather information or gain access to computer systems via the web.
Source: http://www.tradearabia.com/news/IT_144956.html

33. *June 11, ZDNet Blogs* – (International) **Proof of Concept "carpet bombing" exploit released in the wild.** In what appears to be an attempt to provoke Apple to reconsider its currently passive position on the severity of the dubbed as "carpet bomb" flaw, a working Proof of Concept exploit code has been released at a security blog. Safari for Windows puts downloads automatically to Desktop, which can potentially make a mess of Desktop. The security blog also mentions a new security threat in Safari for Windows, different than the "blended threat" described by Microsoft, and summarizes the whole fiasco about who is responsible for what: "Safari for Windows puts downloads to Desktop by default without a dialog box (such as the "File Download" dialog box in IE). Well, this is in fact a quite reasonable and convenient feature - downloading and saving requested file to user's Desktop by default. This feature itself does not constitute a mistake. What really makes the "blended threat" is some problem in loading program library files (DLL) by Windows Internet Explorer (and probably others)."
Source: http://blogs.zdnet.com/security/?p=1264

34. *June 11, Associated Press* – (International) **Virus may be an extra on new high-tech gadgets.** Some of today's most popular gadgets are landing on store shelves with some unwanted extras from the factory – pre-installed viruses that steal passwords, open doors for hackers and make computers spew spam. Computer users have been warned for years about virus threats from downloading suspicious files and opening suspicious e-mail attachments. Now they run the risk of picking up a digital infection just by plugging a new product into their PCs. Recent cases reviewed by the Associated Press include some of the most widely used tech devices: Apple iPods, digital picture frames sold by Target and Best Buy stores and TomTom navigation gear. In most cases, Chinese factories – where many companies have turned to keep prices low – are the source.
Source: http://detnews.com/apps/pbcs.dll/article?AID=/20080611/BIZ04/806110327

35. *June 10, Redmond Channel Partner* – (National) **Microsoft releases 7 patches, 3 critical.** Microsoft released seven patches for its June rollout of security fixes. As expected, three are labeled "critical," three "important" and one "moderate." In total, the patches address about 10 separate vulnerabilities. All of the critical items plug holes vulnerable to remote code execution (RCE) exploits in Windows programs interacting with wireless protocol using voice and data for Bluetooth, Internet Explorer and Microsoft DirectX, an application programming function in Windows. Meanwhile, the important fixes are designed to block elevation of privilege and denial of service from would-be hackers in Windows Internet Name Service, Active Directory and Pragmatic General Multicast, a transport protocol in Windows programs used for file transfer and streaming media. The moderate patch applies to the kill bit function in Windows

programs, a method by which a user can shut off an ActiveX control in IE. But it is the Bluetooth vulnerability, experts say that is most important to patch because it exemplifies the relatively nascent attack vector of wireless peripherals. “[The Bluetooth vulnerability] is noteworthy because user interaction is not required,” said a senior research manager for Symantec. “All that is required is for the device to have Bluetooth on and to be within range of the attacker. That’s something IT guys should look at first.”
Source: http://rcpmag.com/news/article.aspx?editorialsid=9949

Internet Alert Dashboard

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

Communications Sector

36. *June 10, Vermont Public Radio* – (Vermont) **State government demands explanation for Internet outages.** State government demanded an explanation on Tuesday for a series of outages that knocked out Internet service across Vermont. Vermont’s Public Service Commissioner O’Brien made the demand in a formal letter to Level 3 Communications, the Colorado company that operates a the telecommunications network. There has been a failure in the Level 3 network three times in the past three weeks, including an outage of about a half hour Tuesday. The failures made it impossible for customers to access the Internet or make long-distance telephone calls unless they had a backup. The Commissioner says one of the state’s major concerns is the apparent lack of redundancy in Level 3’s network. He says it should have backup systems that would kick in when a problem crops up.
Source: http://www.vpr.net/news_detail/80894/

37. *June 10, WRAL 5 Raleigh* – (North Carolina) **Wilson residents get access to city-owned network.** Wilson residents began signing up for community-provided internet, cable and phone service Tuesday. Over the past few years, the city has installed hundreds of miles of fiber-optic lines to create a network that competes with Time Warner. Wilson officials believe high-speed Internet technology is crucial to attracting new businesses. Soon the city will offer high-speed Internet, phone service and cable TV to any business or home in the city limits. Wilson officials said the fiber-optic network will be self-supportive and use no tax money. Only residents who choose to subscribe will pay for the system.
Source: http://www.wral.com/news/local/noteworthy/story/3022343/

[Return to top]

Commercial Facilities Sector

38. *June 11, Cape Coral Daily Breeze* – (Florida) **Cape bomb scare is false alarm; Official: 'Suspicious package' is woman's misplaced suitcase**. A Cape Coral shopping plaza was evacuated Wednesday evening as police and fire crews and the Cape Coral bomb squad responded to a suspicious package in the parking lot. That package, it turns out, was a misplaced suitcase, officials said. According to a spokesperson, the plaza was evacuated and the area was secured. The bomb squad showed up to handle the 'package' and its then unknown contents. The suitcase, which was filled with computer equipment, was returned to its owner.
Source: http://www.cape-coral-daily-breeze.com/news/articles.asp?articleID=19098

[Return to top]

National Monuments & Icons Sector

39. *June 10, KPHO 5 Phoenix* – (Arizona) **Park exhausts leads in stolen petroglyph.** Kaibab National Forest managers said they have exhausted leads and ask for the public's help for information leading to the recovery of a petroglyph stolen in August 2007. A 4-by-2-foot rock panel covered in images was taken from the site outside of Ash Fork. The panel is one of many in the area from the Western Archaic Period, said a Kaibab National Forest archaeologist. The forest contains more than 9,000 identified archaeological sites, the park Web site said, placing it in the top five forests nationwide in terms of the number of recorded sites. In March 2007, Arizona Site Steward volunteers took photographs of the Ash Fork archaeological site, a Kaibab National Forest archaeologist said. When they returned in August, the rock panel was missing. A Kaibab National Forest archaeologist said vandals have caused other damage nearby. People are illegally harvesting lichen-covered surfaces of rocks for decorative purposes, he said. Authorities said they fear additional vandalism to the archaeological site may occur in the future.
Source: http://www.kpho.com/news/16562837/detail.html

[Return to top]

Dams Sector

40. *June 11, Associated Press* – (Indiana; Iowa) **Sandbagged levee holds in Iowa, protects city.** A sandbagged levee was preventing a swollen river in Cedar Falls, Iowa, from rising out of its banks and flooding the city on Wednesday, but officials asked for extra volunteers to help shore it up as more rain moved across the state. The Cedar River had been expected to top the levee during the night and deluge downtown Cedar Falls. But a city spokeswoman said early Wednesday that the sandbags appeared to be holding. In Elnora, Indiana, berms of white sandbags and concrete barriers held back the White River. Most residents left after voluntary evacuation orders came late Monday, two days after the area got up to 10 inches of rain. Down river from Elnora, a levee failed early Wednesday near the town of Capehart, and Daviess County authorities urged residents to evacuate. Authorities also ordered as many as 300 residents north of nearby Maysville

to evacuate late Tuesday after water topped a levee. Along the Mississippi River, the National Weather Service on Tuesday predicted crests of 10 feet above flood stage and higher over the next two weeks. Most of the towns are protected by levees, but outlying areas could be flooded.
Source:
http://news.yahoo.com/s/ap/20080611/ap_on_re_us/severe_weather;_ylt=AiQ.k1DqH0LHgp7Jj6LPrDas0NUE

41. *June 10, Gazette* – (Iowa) **Coralville Lake tops spillway, Corps now has no control.** Water started flowing in earnest over the Coralville Lake spillway just after 9 p.m. Tuesday, and U.S. Army Corps of Engineers’ officials now say they have no control over the lake’s outflow. The spillway is at 712 feet above sea level. The lake’s level was 712.12 feet by 11 p.m. The lake’s release rate is 20,000 cubic feet per second, up from 18,000 cubic feet per second on Monday. “The gates are wide open,” Coralville Lake operations manager said about the release gates at the dam holding water back in the flood-control reservoir. But water was flowing into the flood-control reservoir at a rate of 21,800 cubic feet per second Tuesday. And the lake’s crest has been adjusted upward slightly today to 715.7 feet above sea level.
Source:
http://www.gazetteonline.com/apps/pbcs.dll/article?AID=/20080610/NEWS/22224431

[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 NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 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

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.