Department of Homeland Security Daily Open Source Infrastructure Report for 4 June 2008

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

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

- According to Reuters, a recently released report of the 2007 underground collapse of the Crandall Canyon coal mine in Utah, which resulted in the deaths of six miners and three rescuers, covered 50 acres. This is about four times larger than the initial estimate made shortly after the disaster. (See item 7)
- The Washington Post reports that a criminal group that specializes in deploying malicious software to steal banking data is presenting victims with fake maintenance pages and error messages as a means of getting around anti-fraud safeguards erected by many banks. It is estimated that this latest scam was sent to around 6,000 to 8,000 targets, and at least 690 people fell victim to it. (See item 14)

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 3, Bloomberg* – (International) **Norway oil producers say rig strike can be averted.** Norway oil producers are "optimistic" a strike called by rig managers this weekend that threatens to cut nine percent of the country's output can be averted as government-mediated talks start on June 5. "We've presented them with a good offer and it should be possible to come to an agreement," the head negotiator for the

Norwegian Oil Industry Association said Tuesday. The Norwegian Organization of Managers and Executives said it will pull 86 workers from StatoilHydro ASA's Snorre A platform and Royal Dutch Shell Plc's Draugen A rig on June 7 if a new agreement is not reached on wages and working hours. The strike imperils output of 220,000 barrels of oil per day. Talks between the union and the industry group, which represents Statoil, Shell, and ConocoPhillips, broke down on May 20. The union has also threatened to broaden the strike to other North Sea platforms after June 7.
Source:
http://www.bloomberg.com/apps/news?pid=20601072&sid=aGWLFTviMT2E&refer=energy

2. *June 3, Bloomberg* – (Texas) **Motiva Texas refinery to restore output in 'couple of days.'** Motiva Enterprises LLC, a joint venture of Royal Dutch Shell Plc and Saudi Arabia's state oil company, said it expects its Port Arthur, Texas refinery to return to full production capacity in the "next couple of days." Power to the refinery, Motiva's largest in the U.S., has been "reestablished" since a blackout at 11 a.m. Monday caused the plant to shut down, a Shell spokesman said. "Products will continue to be supplied from inventory that is on hand," he said. The power disruption was caused by an internal electrical system malfunction. Five workers taken to a hospital for symptoms including heat exhaustion have been released.
Source:
http://www.bloomberg.com/apps/news?pid=20601072&sid=aDrkA7H1TODM&refer=energy

3. *June 3, Juneau Empire* – (Alaska) **Hydroelectric power back in business.** Juneau's hydroelectric power has been restored. The city is no longer running on costly diesel. A spokesman for Alaska Electric Light & Power Co. said the power was back online at 9:17 p.m. Sunday. The city has run on diesel since April 16, when avalanches destroyed the transmission line from the Snettisham hydroelectric project, which ordinarily supplies most of Juneau's energy. All of Juneau will be free from the 52-cent per kilowatt-hour rate by June 15.
Source: http://www.juneauempire.com/stories/060308/loc_285841675.shtml

4. *June 3, Daily Item of Lynn* – (Massachusetts) **State Police Anti-Terror Unit probes LNG incident.** A Russian national was arrested Friday after he was caught taking photographs of the secured liquefied natural gas terminal on Lynn Harbor, touching off an investigation by the state's Anti-Terrorism Task Force, police said. Police say the man allowed officers to search through his backpack and found several pieces of photographic equipment. Though it is not illegal to take pictures in public, police say the man was taking photographs while standing in a posted "no trespassing" area. He was arrested and charged with trespassing. Due to the suspicious nature of the incident, a report of what happened was forwarded to the State Police Anti-Terrorism Unit for further investigation, according to a police spokesman. Employees of National Grid, the company that owns the 12-million gallon gas tank, called police after noticing the alleged suspicious behavior at about 11 a.m., police said.
Source: http://www.itemlive.com/articles/2008/06/03/news/news05.txt

5. *June 2, Reuters* – (National) **Energy Dept creates wind-turbine research group.** Six leading wind turbine manufacturers signed an agreement with the U.S. Department of Energy (DOE) to find ways to improve turbine design and production methods as the industry attempts to boost its contribution to the nation's electric supply, the energy agency said on Monday. The memorandum calls for a two-year collaboration to research methods to design and fabricate more reliable turbine components; reduce installation and operating costs; address environmental and technical issues; and to develop turbine certification, workforce, and grid connection standards. The DOE assistant secretary of energy efficiency and renewables said the cooperative research effort between the agency and industry shows a "shared commitment" to expand wind's share of the U.S. electric supply from about two percent to a 20 percent target by 2030.
   Source: http://www.reuters.com/article/marketsNews/idUSN0231271020080602

6. *June 2, Dallas Morning News* – (Texas) **PUC expects record electricity demand, asks Texans to conserve.** The Public Utility Commission (PUC) expects record-high electricity demand this month and advises Texans to conserve. The commission boosted its conservation alert to yellow because of forecasts for hotter-than-normal temperatures this week. The commission said Monday in a news release that the state should have adequate electricity.
   Source: http://www.dallasnews.com/sharedcontent/dws/news/texassouthwest/stories/060308dnbuselectric_demand.53e2ae90.html

7. *June 2, Reuters* – (Utah) **Fatal Utah coal mine collapse covered 50 acres.** The 2007 underground collapse of the Crandall Canyon coal mine in Utah, which resulted in the deaths of six miners and three rescuers, covered 50 acres, according to a report released on Monday by seismologists. According to the University of Utah Seismograph Stations, new calculations show the estimated size of the collapse, which registered as a 3.9 magnitude earthquake, is about four times larger than the initial estimate made shortly after the August 2007 disaster. "The collapse probably happened within just a few seconds and was not a long, drawn-out affair," said a University of Utah seismologist and lead author of the study. Seismologists insisted from the day of the collapse that the magnitude-3.9 seismic event was the mine collapse itself. The owner of the mine, which has ceased operation, argued it was a natural quake that triggered the collapse. The report has been submitted to the journal Seismological Research Letters and to federal Mine Safety and Health Administration investigators.
   Source: http://www.reuters.com/article/domesticNews/idUSN0229588120080602

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

8. *June 3, Associated Press* – (International) **U.S., Turkey reach nuclear energy deal.** The U.S. and Turkey are moving toward cooperation on civilian nuclear technology. The U.S. State Department says the two countries concluded a deal that would allow them to exchange nuclear technology, material, and reactor equipment. A U.S. State Department spokesman said Monday that the deal would boost nuclear energy development and enhance security. The agreement must be submitted to the U.S. Congress, which would have 60 working days to block it with legislation if it objects.
   Source: http://www.iht.com/articles/ap/2008/06/02/america/NA-GEN-US-Turkey.php

9. *June 3, Associated Press* – (Nevada) **Nevada nuclear dump application filed.** The Bush administration moved a step closer to building a nuclear waste dump at Yucca Mountain in Nevada on Tuesday, filing a formal application for a construction license. The U.S. Energy Department sent the application to the U.S. Nuclear Regulatory Commission, which will have three years to review it.
   Source: http://www.lvrj.com/breaking_news/19489014.html

10. *June 3, Press of Atlantic City* – (New Jersey) **Shieldalloy decommissioning called too slow.** A federal board criticized the slow pace of decommissioning a radioactive site in Newfield as "unacceptable." In a June 2 report, the Atomic Safety and Licensing Board faulted the review of the Shieldalloy site, a former factory that maintains a radioactive slag pile on its grounds. The facility processed ore until 1998, but a final plan for decommissioning is not expected to be ready until 2011.
    Source: http://www.pressofatlanticcity.com/182/story/173409.html

[Return to top]

Defense Industrial Base Sector

11. *June 2, Associated Press* – (National) **Navy sees spying, not flying, future with drones.** The Air Force and Navy have contrasting visions for the next generation of America's air arsenal point. The debate continues within the military about the pace of incorporating remote-control technology into future battle strategies. The Navy resists substituting fighter pilot training and instincts with aircraft guided by operators who can be thousands of miles away. For the moment, the Navy is deeply committed to plans for the F-35 fighter jet and developing a drone fleet strictly for surveillance and other non-weapon tasks. However, the Air Force has used armed drones for years and appears to embody Pentagon trends to encourage drones as a way to reduce costs and consolidate personnel. The U.S. Defense Secretary called on the Air Force and other military officials to rethink "long-standing service assumptions and priorities about which missions require certified pilots, and which do not." The secretary added that "unmanned systems cost much less and offer greater loiter times than their manned counterparts, making them ideal for many of today's tasks."
    Source: http://www.msnbc.msn.com/id/24936039/

[Return to top]

Banking and Finance Sector

12. *June 3, Dark Reading* – (National) **Chinese hacker behind US Court, IRS scams.** SecureWorks Inc., a security services provider, reported Tuesday that a Chinese hacker is behind the current and former executive "whaling phishing scams" involving the U.S. Federal Courts and the Internal Revenue Service. The Director of Threat Intelligence for SecureWorks discovered this past weekend's U.S. Tax Court scam whereby corporate financial executives are receiving phishing emails with subjects like "Notice of Deficiency" purporting to be from the United States Tax Court. The emails state that the recipient has a case pending with the Internal Revenue Service. Links in the phishing email lead to a download page for a Trojan known alternately as DlRhifrem, Rhifrem, and Fireming. It is a spyware BHO masquerading as an Adobe Acrobat ActiveX control. Additionally, in this latest scam, the hacker is targeting C-Level financial executives with information from non-public databases, such as those found in legal databases, ie: direct phone numbers, company addresses, titles, etc. SecureWorks has determined that the hacker behind the U.S. Tax Court and the IRS scams is Chinese, most likely from Hong Kong or Taiwan, and has had first-hand experience with the U.S. courts system. The hacker is technically savvy and has the capability to modify the trojan to do what they want it to do and understands social engineering tactics. This is the same variant of the DIRhiferm malware that was used in the "U.S. Courts" attack which took place in mid April of this year. However, this is the first time a root certificate has been included into the whaling scam.
Source: http://www.darkreading.com/document.asp?doc_id=155416&WT.svl=wire_1

13. *June 3, vnunet.com* – (National) **Spammers exploit Google Docs.** Spam levels jumped in May to 76.8 per cent of all emails sent globally, according to new monitoring data. MessageLabs' latest Intelligence Report attributed this hike to a change of tactics in which spammers are moving away from a reliance on email attachments. In addition to the variety of new spam techniques, MessageLabs also identified several new phishing exploits this month, including one which preyed on a bank's environmentally-conscious customers. Using the Srizbi botnet to launch the attacks, the phishers took advantage of a 'Go Green' campaign run by Central Bank in Missouri to lure recipients into sharing their bank details in order to register for electronic statements. Also in May, MessageLabs found evidence of phishing attacks claiming to be from HSBC bank which purported to be a secure connection via HTTPS. Closer inspection revealed that the attack was actually a standard HTTP link to a domain pretending to be the actual bank.
Source: http://www.vnunet.com/vnunet/news/2218111/spammers-exploit-google-docs

14. *June 2, Washington Post* – (National) **Beware of error messages at bank sites.** A criminal group that specializes in deploying malicious software to steal banking data is presenting victims with fake maintenance pages and error messages as a means of getting around anti-fraud safeguards erected by many banks. Dozens of banks now require business customers to log in to their accounts online using so-called "two factor authentication" methods, which generally require the customer to enter something in addition to a user name and password, such as a random, one-time-use numeric code

generated by a key fob or a scratch-off pad. But one of this past year's most prolific cyber gangs has devised a simple but ingenious method of circumnavigating these security measures. When a victim whose PC is infected with their data-stealing malware attempts to log in at a banking site that requires two-factor authentication, the fraudsters modify the display of the bank site in the victim's browser with an alert saying "please allow 15 to 30 minutes for your request to be synchronized with our server." By intercepting the victim's password along with the one-time code - and assuring that the victim will never be able to use that one-time code - the thieves can quickly use the one-time code to log in as the victim and proceed to drain the bank account. According to researchers at iDefense, this tactic was most recently used in an attack nearly two weeks ago, in which the fraudsters sent thousands of targeted e-mails spoofing the United States Tax Court. The message in the email prompts the recipient to click on a link to view the complaint. Those who do so are greeted with a prompt to install an Adobe Acrobat viewer. Of course, the program is not a viewer at all, but a "browser helper object" (BHO) that allows the attacker to steal passwords and data when victims log on to encrypted (https://) Web sites. More importantly, the BHO lets the attackers modify Web pages that the victim sees in real time. As a result, when victims are presented with one of these error pages, the message is inserted into the body of the bank's actual Web page. In such an attack, even an alert victim is unlikely to notice anything amiss. The director of rapid response at iDefense said the criminal group responsible for this and a string of other such targeted attacks use the fake scam message for customers of roughly 50 different financial institutions that deploy two-factor authentication for business customers. iDefense estimates this latest scam was sent to around 6,000 to 8,000 targets, and the company has evidence that at least 690 people fell victim to the scam.
Source:
http://blog.washingtonpost.com/securityfix/2008/06/beware_of_error_messages_at_ba_1.html?nav=rss_blog

[Return to top]

Transportation Sector

15. *June 2, Associated Press* – (National) **Airports focus on 'security that you can't see'.** New and renovated airports have poured millions of dollars into safety upgrades since the September 11 terrorist attacks, working advice from explosives experts into design plans that encompass everything from the most secure place for parking garages to more efficient security checkpoints. But many other upgrades fly beneath passengers' radar. In Indianapolis, those steps include the bollards, windows that will fold like a drape when broken rather than exploding into shards of flying glass, and a 240-foot-wide strip of lawn that will separate the front entrance of the new terminal from its five-story parking garage. Planners generally use bollards or cement piers to keep possible bomb-laden cars at least 20 feet to 30 feet from a building's support beams, said a senior adviser with Airports Council International-North America. The Indianapolis terminal is one of the first airports designed and built since September 11. Planners more than doubled the space provided for security equipment compared with the current airport. They added a room for isolating international travelers suspected of

carrying a contagious disease. They also spent $24 million to build an inline baggage screening system beneath the terminal's main floor. The system includes about a mile of conveyor belts that feed luggage through scanners, which compare bag contents with properties found in explosives. Security personnel will keep watch from a nearby room, and they will be able to quickly divert any suspicious bags.
Source:
http://news.yahoo.com/s/ap_travel/20080602/ap_tr_ge/travel_brief_airports_secure_design;_ylt=AplyzR4zw965iV5jdL0_nsCs0NUE

16. *June 2, Associated Press* – (Texas) **Jet's broken window leads to emergency landing.** An American Airlines jetliner made an emergency landing after a pane from a cabin window shattered during a flight and the shards of glass disabled an engine. The outside pane of the triple-pane window broke about 20 minutes after the takeoff from Dallas-Fort Worth International Airport. There was no pressure loss in the cabin and none of the 132 people aboard the Fort Myers, Florida-bound flight was harmed Sunday, an American Airlines spokesman said. Asked about the cause of the break, he said, "We don't really know. Just repeated pressurization can put stress on the window without breaking. That is fairly unusual."
Source: http://ap.google.com/article/ALeqM5ic-MGLIkmZt8iJbKCT9RgqEm-MHQD9123MA00

17. *June 2, Web User* – (National) **Suspect airline parts flood the net**. Questionable aircraft components, including valves, gears and radar parts are being sold in bulk over the web, according to research. MarkMonitor's Spring 2008 BrandJacking Index revealed that the black market for airline parts remains healthy with the internet presenting a lucrative channel for unscrupulous traders. In general, vendors from the U.S. and China are responsible for selling the uncertified aircraft parts. The findings come in the wake of last week's prosecution in the U.S. of a budget airline for endangering the safety of passengers after allowing a 757 jet to fly "illegally" to America with faulty gauges. Counterfeit components have in the past turned up on U.S. military and NATO aircrafts, NASA space shuttles and even Air Force One, the plane used to fly the U.S. president. The report, which looks at how leading brands are attacked online, also found that there is a proliferation of online auction sites that sell unusable airline vouchers to cheat consumers out of their money while infecting their computers with spyware.
Source: http://www.webuser.co.uk/news/news.php?id=257558

[Return to top]

Postal and Shipping Sector

18. *June 3, Wall Street Journal* – (International) **Banned by Beijing: It's in the mail.** China is continuing apace with stepped-up security measures ahead of this summer's Olympic Games. Xinhua reports today that China's postal service will not accept mail containing liquids and "a few other materials" from June 1 to October 31. Those other materials include "all kinds of chemical products, powder goods, unidentified metal, mechanical, and electrical products [and] sealed containers with unidentified gas or

liquid," the report said, though packages containing those items can still be mailed if the sender first obtains a safety certificate from local police. The postal service is also increasing inspections of mail sent to the Olympic co-host cities in mainland China, in addition to the main host city of Beijing.
Source: http://blogs.wsj.com/chinajournal/2008/06/03/banned-by-beijing-its-in-the-mail/?mod=googlenews_wsj

[Return to top]

Agriculture and Food Sector

19. *June 3, Packer* – (New York) **New York leads way in national food safety program.** New York officials say the state is the first one to achieve national Food and Drug Administration food safety standards. The state's governor said the Empire State has become the first among five states the FDA asked to adopt a national food safety program. The governor also stated that the Manufactured Food Regulatory Program Standards should help safeguard the state's food supply. By completing the program before other states, New York's standards remain on par with federal standards, he said. Those standards, said to be more uniform, include measurement and evaluation of food manufacturing, processing, packing, or handling, the governor said.
Source: http://thepacker.com/icms/_dtaa2/content/wrapper.asp?alink=2008-174835-934.asp&stype=topstory&fb

20. *June 2, United Press International* – (National) **Worker attitude affects food safety.** Researchers from Kansas State University surveyed 190 food service employees in 31 restaurants across three Midwestern states on their knowledge of, and attitude toward, three food safety measures that have the most substantial impact on public health: hand washing, using thermometers, and proper handling of food contact surfaces. Only employees whose jobs directly involved food preparation tasks participated. Food service workers' attitudes toward safety practices have a direct effect on food-borne illnesses in restaurants, U.S. researchers say. The study, published in the Journal of the American Dietetic Association, said that providing workers with training that does not target their attitudes may not improve food safety results.
Source:
http://www.upi.com/NewsTrack/Health/2008/06/02/worker_attitude_affects_food_safety/3807/

21. *June 2, Kansas City infoZine* – (International) **Abbott recalls infant formula.** Abbott has announced an international recall of certain lots of infant formula because air may have entered the cans, resulting in oxidation. Consumption of highly oxidized foods can lead to gastrointestinal symptoms such as nausea, vomiting and diarrhea, the U.S. Food and Drug Administration said.
Source: http://www.infozine.com/news/stories/op/storiesView/sid/28688/

22. *June 2, KNTV 11 San Jose* – (National) **Scientists argue apple moth spray plan won't work.** The battle is heating up over a controversial plan to start spraying for the light brown apple moth. But the scientific community is divided over whether the plan to use

aerial spraying to control the apple moth population will actually work. A group of prominent University of California Davis scientists have written a letter warning that California's plan to eliminate the bug will not work. "There's some mountains that can't be moved and there's some insects that can't be eradicated and this is simply one of them and so you need a reality check here," said a UC Davis entomologist. The three scientists who drafted the letters are entomologists. Aerial spraying against a multibillion dollar invasive pest has become an intensely political issue, but scientists working for the state are convinced it will be both safe and effective and so the campaign is set to begin. "We think it will work," an employee of the Department of Food and Agriculture. "The trials that we've seen in New Zealand using this technique have shown excellent results."
Source: http://www.nbc11.com/news/16466172/detail.html

[Return to top]

Water Sector

23. *June 3, Examiner* – (Maryland) **Fats, oils, grease pose threat of sewage spills.** What might have looked like harmless leftover grease tossed down the drain sparked a more than 500,000-gallon sewage overflow earlier this year in Laurel, Howard officials said. Now officials are warning residents that pouring oil and grease down the drain is a major cause of sewage backups and has caused about half of the spills. Fats, oils, and grease caused seven of the 14 overflows in Howard in 2007, according to Maryland Department of the Environment (MDE) data. Local jurisdictions notify MDE of every spill, and in Howard, the public is notified anytime a spill affects a waterway. In Anne Arundel, grease caused four spills, totaling more than 9,000 gallons. Spills caused by fats, oils, and grease tend to be higher-volume spills – in the tens of thousands of gallons rather than a few hundred, said Howard's utilities chief, adding he was not sure why the volume was higher.
Source: http://www.examiner.com/a-1421289~Fats__oils__grease_pose_threat_of_sewage_spills.html

24. *June 3, Environmental Protection Agency* – (Missouri) **EPA signs record of decision on West Lake Landfill Superfund Site in Missouri.** Installations of a multi-layered engineered cover and a system of new monitoring wells are among a series of key remedial actions that will best serve to protect groundwater resources and human health at the West Lake Landfill Superfund Site in Bridgeton, Missouri, according to a plan formally approved recently by the Environmental Protection Agency (EPA). "We believe it is imperative to move ahead by placing a properly engineered cover on the landfill," an EPA regional administrator said. "The cover would serve as a stable barrier to minimize future exposure to waste material, as the landfill currently has no such protective cap." EPA's design process also calls for the installation of a new system of monitoring wells around the site, and for long-term groundwater sampling to occur, with the results of all tests to be made available to the public. The Agency's next steps for West Lake Landfill will be to work closely with the site's owners and responsible parties as they identify and secure the services of various contractors to develop specific engineering designs, construct the landfill cover, install the monitoring wells, and

establish specific schedules and measures for sampling procedures and sharing test results.
Source: http://www.wateronline.com/article.mvc/EPA-Signs-Record-Of-Decision-On-West-Lake-0001?VNETCOOKIE=NO

25. *June 2, Rocky Mountain News* – (Colorado) **High-stakes water trial on hold.** A critical water trial in Wray, Colorado, which threatened closure of more than 1,300 high-capacity irrigation wells, has been postponed one week while parties consider a proposed $20 million settlement of the case. Nearly 4,000 powerful irrigation wells provide the backbone of a booming ethanol economy on the eastern plains. But pumping from the wells has been shown to depress flows in the Republican River, leaving less surface water for farmers who rely on the river for irrigation. Under this settlement, special districts that represent well users would likely issue bonds to pay the settlement to the surface water right-holders, using new tax revenues to pay off the bonds. The agreement must be approved by several other entities, as well, and ultimately might have to go to a vote of Yuma County residents.
Source: http://www.rockymountainnews.com/news/2008/jun/02/high-stakes-water-trial-warring-parties-seek-settl/

26. *June 2, Chattanooga Times Free Press* – (Tennessee) **Sewer challenges spread across Tennessee.** Hamilton County's Water and Wastewater Treatment Authority has to clean up its act, according to an order from state environmental regulators. The local system is in the same category as sewer authorities in Knoxville, Nashville, Memphis' Shelby County, and many areas in between. Data provided by the department show that 68 publicly owned treatment works in Tennessee are under some type of order to get their systems up to standards. A Tennessee Advisory Commission on Intergovernmental Relations study released in March noted that many systems are on their last legs. "Many sewer lines are 40 to 50 years old or older and are approaching the end of their useful lives," states the executive summary of the study, titled "Corroding and Failing Sewer Lines: How Big a Problem?" Increasing populations also are a factor, according to the report, because many systems were built before the rapid growth during the past couple of decades. The Tennessee Department of Environment and Conservation's order against Hamilton County's treatment authority cites the authority for dumping excess water from the Signal Mountain Sewage Treatment Plant into the Tennessee River. The order carries a $25,000 fine and $232,000 in possible additional fines. The plant was taking in more than it could handle during big rains, authority officials have said.
Source: http://timesfreepress.com/news/2008/jun/02/sewer-challenges-spread-across-state/?local

27. *June 2, Atlanta Journal-Constitution* – (Georgia) **Lake Lanier gets to keep more water.** The operators of Buford Dam at Lake Lanier received approval Monday to hold onto more water for metro Atlanta. The U.S. Fish and Wildlife Service concluded that a proposal for Lake Lanier and other Chattahoochee River reservoirs to store more water and release less will not be a threat to endangered and threatened fish and mussels downstream. The U.S. Army Corps of Engineers' put the plan, a response to north Georgia's continuing record-breaking drought, into effect Sunday. Previously, the five

reservoirs were permitted to store 30 percent of the inflow into the river basin. The proposal, announced in April, bumps the storage rate to 50 percent. The Fish and Wildlife Service determined that the additional retention, while it will have adverse effects on Gulf sturgeon and three varieties of mussel in the Apalachicola River and bay that are either endangered or threatened, will not jeopardize their existence. The Atlanta Regional Commission's environmental planning director said Monday the plan is not enough. Some down river in Florida are not very happy, either. "A continued reduction in flows to the Apalachicola River over the next five years places the economic and environmental future of an entire region at risk," said Florida's governor.
Source:
http://www.ajc.com/metro/content/metro/stories/2008/06/02/lake_lanier_water.html

[Return to top]

Public Health and Healthcare Sector

28. *June 3, Agence France-Presse* – (International) **Mystery epidemic hits NKorea: aid group.** A mystery epidemic spreading along some North Korean border towns with China has claimed the lives of dozens of children, Good Friends, a Seoul-based humanitarian group, said Tuesday. The highly contagious disease has sparked a health alert with an estimated five or six children dying every day since April 27 in the northeast city of Hoeryong, the group said. North Korean health authorities have been unable to stop the spread of the epidemic or to come up with an exact diagnosis or cure, it added. Doctors in the North suspect it may have been caused by avian influenza or hand-foot-mouth disease. "Bird flu is spreading," the group quoted one doctor as saying. The group quoted another doctor as saying hand-foot-mouth disease could be spreading from China, where it has killed several dozen children. The outbreak is spreading mainly among state-run child daycare centers and kindergartens and no cases of adult infections have been reported, the doctor said.
Source:
http://news.yahoo.com/s/afp/20080603/hl_afp/nkoreahealthchildren;_ylt=AjgpW4h.4j6pPVhmetauppfVJRIF

29. *June 3, Associated Press* – (National) **Walter Reed says patient data may be compromised.** Sensitive information on about 1,000 patients at Walter Reed Army Medical Center and other military hospitals was exposed in a security breach, sparking identity theft concerns and an investigation by the Army. Names, Social Security numbers, birth dates and other data were released, hospital officials said Monday. The computer file that was breached did not include information such as medical records or the diagnosis or prognosis for patients, they said. The disclosure marked the latest in a series of breaches of government computer records. Walter Reed officials declined to explain exactly how the information was compromised, pending an ongoing investigation by the hospital and the Army. They would only say that the computer file was found on a "non-government, non-secure computer network."
Source:
http://ap.google.com/article/ALeqM5ggIYzqvXf4Qosf6ubPXxZRRAMPEAD9127N4O0

30. *June 2, Center for Infectious Disease Research & Policy* – (National) **USDA releases sequences of 150 avian flu viruses.** The U.S. Department of Agriculture (USDA) recently announced the release of complete genetic data for 150 avian influenza viruses in an effort to connect genetic information with the biological effects of the viruses and to improve diagnostic tests. USDA announced the release of the viral genetic sequences to GenBank, the National Institute of Health's public genetic sequence database, on May 30. The viruses, mostly from North America, represent nearly all avian flu subtypes and were collected from the 1930s to the present, according to the research leader of the Exotic and Emerging Avian Viral Diseases Research Unit at the Southeast Poultry Research Laboratory (SEPRL) in Athens, Georgia. The lab is part of the USDA's Agricultural Research Service.
Source:
http://www.cidrap.umn.edu/cidrap/content/influenza/avianflu/news/jun0208genes.html

[Return to top]

Government Facilities Sector

Nothing to report

[Return to top]

Emergency Services Sector

31. *June 2, Daily World* – (Louisiana) **Storm readiness urged.** Cleco Corp., an energy provider that services about 17,000 St. Landry Parish customers, met with emergency first responders Monday in Eunice to discuss safety preparations and power restoration for the 2008 hurricane season. The Atlantic hurricane season officially began Sunday. For the fifth straight year, experts are predicting more storms than usual in the Atlantic basin. Storm forecasters are predicting at least 12 named tropical storms, three or four hurricanes and at least one major hurricane. The engineering company is holding storm meetings throughout south Louisiana. First responders were updated on the company's restoration process after a storm. Cleco representatives are busy trying to get first responders all the information they need. At the same time, first responders are urging citizens to prepare.
Source:
http://www.dailyworld.com/apps/pbcs.dll/article?AID=/20080603/NEWS01/806030307/1002

32. *June 2, CFNEWS 13 Orlando* – (Florida) **First responders run hurricane drill this week.** State emergency workers began a drill Monday involving a fake hurricane named Herb, modeled after a Category 3 storm that barreled into Florida in 1896. Personnel from National Guard directors to state weather forecasters manned their stations, which were equipped with new computers and better communications gear. After a couple of quiet years, emergency managers said it was more important than ever. "Hurricanes are kind of a rare thing. It's just, when they hit, if you're not ready, it

could cost you your life, it could cost you your home, and a lot of other things that are valuable to you," said the director of the Florida Division of Emergency Management. "Our challenge every year is to remind people is how serious the threat is." The drill is scheduled to run through Thursday.
Source:
http://www.cfnews13.com/Weather/HurricaneCenter/2008/6/2/first_responders_run_hurricane_drill_this_week.html

[Return to top]

Information Technology

33. *June 3, vnunet.com* – (International) **Spammers exploit Google Docs.** Spam levels jumped in May to 76.8 percent of all emails sent globally, according to new monitoring data. MessageLabs' latest Intelligence Report attributed this hike to a change of tactics in which spammers are moving away from a reliance on email attachments. Spammers are instead moving towards the exploitation of free mainstream hosted services such as Google Docs, Google Calendar and Microsoft SkyDrive. "The savvy and accurate cyber-criminals of today seem to have abandoned the attachments tactic that was so innovative in late 2007 and are exploiting free hosted applications which have become mainstream in 2008," said the chief security analyst at MessageLabs. "The spammers are taking advantage of the fact that these services are free, provide ample bandwidth and are rarely blacklisted," he said, adding, "This is one more addition to the growing list of ways in which the spammers have succeeded in outsmarting traditional detection devices." MessageLabs intercepted spam emails in May which contained links to spam contained in documents hosted on the Google Docs environment. Traditional spam filters do not block links to the Google Docs domain, and spammers are using this to their advantage and even tracking their success through Google Analytics. Spammers are also using Microsoft's SkyDrive shared file hosting service. Spam generated using this technique accounted for one per cent of all unsolicited mail in May.
Source: http://www.vnunet.com/vnunet/news/2218111/spammers-exploit-google-docs

34. *June 3, CNet News* – (International) **Storm worm resurfaces, tries love angle again.** After a hiatus, the gang behind the Storm worm is attempting to exploit people's curiosity about a fictional love interest to tempt users into downloading the malware, according to security training organization the Sans Institute. A security expert from the Sans Institute warned on Tuesday that a Storm worm download site had been detected by security researcher 'DavidF'. A link that contained the site's IP address was being spammed out in emails, he wrote in a blog post. He noted that spam is being sent with the message: "'Crazy in love with you' hxxp://122.118.131.58". He wrote: "I checked that site and could only find an index.html, lr.gif and loveyou.exe." The researcher said that index.html encourages visitors to run the 'loveyou' executable by asking: "Who is loving you? Do you want to know? Just click here and choose either 'open' or 'run'." Loveyou.exe is a version of the Storm worm, also known as Trojan.Peacomm.D by Symantec and Troj/Dorf-AP by Sophos. He recommended IT professionals block the IP address until it gets "cleaned up". The unknown gang behind the Storm botnet tried a similar technique in January in the run up to Valentine's Day. At the time, Sophos

warned that the gang was using a social-engineering technique in an attempt to trick users into clicking on a link in a 'Valentine's Day' email. Storm worm attacks then dropped off, leading some security vendors to report that the influence of Storm worm was waning. However, in May, Symantec researchers warned they had identified a number of nascent Storm worm hosting domains using fast-flux techniques to mask their URLs.
Source: http://news.zdnet.co.uk/security/0,1000000189,39428439,00.htm

35. *June 2, Security Products* – (International) **Study: Risky online behavior more likely to happen at small companies.** Trend Micro recently reported that in the U.S., U.K., Germany and Japan, employees in small companies took more online risks while on the company network compared to their counterparts in larger organizations, according to the results of a study that explores corporate computer users' perceptions of and experiences with security threats. The study, which surveyed usage habits of 1,600 corporate end users in the U.S., U.K., Germany and Japan, found that certain risky activities such as browsing Web sites unrelated to work, making online purchases, visiting social networking sites, downloading executable files and checking personal Web-based e-mail were more likely to take place in small businesses. For example, 32 percent of small business employees in the U.K. have admitted to downloading executable files that can potentially lead to Trojan or virus attacks and, ultimately, identity and data theft. Checking personal e-mail is the most popular non-work related online activity for German workers -- 70 percent of small-business employees do this at work, compared to 59 percent of those in large companies. In Japan, the study revealed that most of the personal Internet activities stated above were more likely to occur in small businesses. Despite a higher level of risky online behavior taking place, only about 50 percent or fewer end users within small companies said they had an IT department which may explain why spam, phishing and spyware were more commonly reported within these companies compared to larger ones.
Source: http://www.secprodonline.com/articles/63564/

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 2, Government Technology* – (International) **"State of the Internet" report released.** Akamai Technologies Inc. last week announced the release of its inaugural "State of the Internet" report. Beginning with the January to March 2008 time period (first quarter), Akamai will be publishing a quarterly "State of the Internet" report extrapolated from data gathered across Akamai's global server network. This report

will include data on the origins of attack traffic, network outages and de-peering events, as well as a look at broadband connectivity by geography. In addition to providing a quarterly summary, Akamai will document trends seen in this data over time.
The report will also aggregate publicly available news and information about notable events seen throughout the quarter, including denial of service attacks, Web site hacks, and network events. During the first quarter of 2008, for example, Akamai observed attack traffic originating from 125 unique countries around the world. China and the United States were the two largest attack traffic sources, accounting for some 30 percent of this traffic in total. Akamai observed attack traffic targeted at 23 unique network ports. Many of the ports that saw the highest levels of attack traffic were targeted by worms, viruses and bots that spread across the Internet several years ago. A number of major network "events" occurred during the first quarter that impacted millions of Internet users. At the end of January, undersea cable cuts in the Mediterranean Sea severed Internet connectivity between the Middle East and Europe, drastically slowing communications. De-peering events between major networks impacted Internet communications for selected Internet users in the United States and Europe for a two-week period. A routing change by a telecommunications provider spread across the Internet resulting in a popular Internet video sharing site to go offline for several hours. The company is planning to release its second quarter "State of the Internet" report in August.
Source:
http://www.govtech.com/gt/articles/366563?utm_source=rss&utm_medium=link

37. *June 2, Computerworld* – (National) **Smartphones 'bigger security risk' than laptops.** Smartphones are seen as a more of a security risk than laptops and mobile storage devices, according to new research. Some 94 percent of senior IT staff fear PDAs present a security risk, just above the 88 percent who highlighted mobile storage devices as a worry. Nearly eight in 10 said laptops were an issue. Only four in 10 had encrypted data on their laptops, and the remainder said the information was "not worth" protecting. The results come from a survey of 300 senior IT staff conducted by endpoint data protection supplier Credant Technologies. A key danger with PDAs was that over half of IT executives surveyed were "not bothering" to enter a password when they used their phone. Nine in 10 of the smartphones were being given access to company networks without extra security, even though the phones were individually owned by users. There were no access restrictions being applied to 81 percent of the phones. Credant Technologies said smartphones had become "easy pickings" for any opportunists trying to steal them and access information.
Source: http://www.networkworld.com/news/2008/060208-smartphones-bigger-security-risk-than.html

[Return to top]

Commercial Facilities Sector

Nothing to report

[Return to top]

National Monuments & Icons Sector

38. *June 2, Center for Biological Diversity* – (California) **U.S. Forest Service rejects environmentalists' appeal of SoCal national forest management plans.** The U.S. Forest Service has rejected a formal administrative appeal by environmentalists of the agency's management blueprint for the four southern California National Forests – the Angeles, Cleveland, Los Padres, and San Bernardino. "Southern California national forests provide an increasingly rare wild refuge for imperiled plants and animals in a growing sea of urban development," said a conservation manager at the Center for Biological Diversity. "Yet the Forest Service ignores these values and treats most of this land as if it were worthy only of development for urban infrastructure, noxious motor recreation, and other exploitation." The forests provide a home for at least 480 at risk species.
    Source: http://www.biologicaldiversity.org/news/press_releases/2008/southern-california-forests-06-02-2008.html

39. *May 31, KCNC 4 Denver* – (New Mexico; Colorado) **4 corners could exceed air pollution levels.** Coal-fired power plants and other pollution sources in the Four Corners area could boost smog levels past federal limits in New Mexico and southwest Colorado this summer, government officials and environment and health care managers warn. Mesa Verde National Park could exceed federal air-quality standards, said participants at an air-quality forum at Fort Lewis College last week. "Very serious air-quality issues need to be addressed, particularly ozone," said an air quality division bureau chief at the New Mexico Environment Department. The Environmental Protection Agency in March tightened the ozone limit to 75 parts per billion, down from the maximum concentration of 80 to 84 parts per billion. The air quality division bureau chief said the region contains seven Class 1 sites, generally national parks or wilderness areas, where the air quality is supposed to be better than in other areas. Other air-quality problems in the area are haze, mercury, and nitrate pollution.
    Source: http://cbs4denver.com/local/Four.Corners.smog.2.737563.html

[Return to top]

Dams Sector

40. *June 1, Associated Press* – (Pennsylvania) **U.S. Army Corps of Engineers reopens Monongahela River lock.** The U.S. Army Corps of Engineers has reopened the main lock chamber of a dam along the Monongahela River near Pittsburgh. The lock chamber in Braddock had been closed since Friday, when officials discovered a broken hinge. It was reopened a day ahead of schedule after repairs were completed. The U.S. Army Corps of Engineers says the closure delayed commercial and recreational traffic on the river, with some tow boats waiting as long as 17 hours to pass through a smaller secondary chamber.
    Source: http://ydr.inyork.com/ci_9447036

[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