Department of Homeland Security Daily Open Source Infrastructure Report for 14 April 2008

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

- According to the Glasgow Daily Record, detailed research on British oil refineries and terminals was found on a computer memory stick at the home of an alleged ringleader of the liquid bomb terror plot, Woolwich Crown Court heard Thursday. Prosecutors said the information on the stick could refer to possible targets. (See item **1**)
- CNN reports sensitive and stolen U.S. military items are being sold on eBay and Craigslist, according to a report by the Government Accountability Office. Government investigators posing as buyers were able to purchase a dozen prohibited military items on the popular online selling sites. (See item **8**)

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. *April 11, Glasgow Daily Record* – (International) **Grangemouth refinery 'was terror bomb plot target.'** Grangemouth oil refinery in Stirlingshire, Scotland, was a possible target for the liquid bomb terror plotters, prosecutors claimed Thursday at Woolwich Crown Court. Detailed research on British oil refineries and terminals was found on a computer memory stick at the home of an alleged ringleader of the plot, the court heard. Prosecutors said the information on the stick could refer to possible targets. Eight Muslim men are on trial accused of plotting to blow up seven transatlantic jets with liquid explosives hidden in soft drink bottles. They deny conspiracy to murder

thousands of passengers. A prosecutor told the jury that the memory stick was found at the home of a defendant in High Wycombe, Buckinghamshire. As well as the Grangemouth site – which sits next to a town of 17,000 people and employs more than 1000 staff – the stick contained details of oil facilities at Fawley in Hampshire, Coryton in Essex, Killingholme on Humberside, and Milford Haven in Wales.
Source: http://www.dailyrecord.co.uk/news/scottish-news/2008/04/11/grangemouth-refinery-was-terror-bomb-plot-target-86908-20378961/

2. *April 11, Bloomberg* – (Southeast) **Enterprise calls force majeure after closing gas line.** Enterprise Product Partners LP declared force majeure after a pipeline leak shut down offshore natural-gas supplies. The declaration was made on April 9, an Enterprise spokesman said Friday. That was the day the company detected a leak on the $286 million Independence Trail pipeline that ships gas from the Independence Hub in the Gulf of Mexico. "The force majeure affects only the producers group, which is headed by Anadarko," he said.
Source:
http://www.bloomberg.com/apps/news?pid=20601072&sid=afX99aqcXqAQ&refer=energy

3. *April 11, KPRC 2 Houston* – (Texas) **44 explosive devices missing since falling off truck.** Nearly four dozen explosive devices owned by Key Energy Services and used in oil field exploration have been missing since they fell off the back of a truck Wednesday near Cleveland, Texas. Liberty County's emergency management officials said the 44 bell-shaped, high-impact devices are very dangerous. "If tampered with, they could explode in your hand like a grenade," said a spokesman. Fifty-two of the devices were in a cooler that fell off the back of a truck along Highway 321 on Wednesday afternoon while being transported out to the field for training, company officials said. The company and several Liberty County agencies have searched a 15-mile stretch for the devices, but only six were found in a ditch. Authorities said they fear someone has taken the other 44 devices because they are valuable. Crews will continue searching for the devices, which are about two inches tall, 1.5 inches wide at the base, and 5.5 inches in diameter. Investigators said they got a tip that someone was seen picking up the cooler and the devices.
Source: http://www.click2houston.com/news/15855134/detail.html

4. *April 10, Dallas Business Journal* – (Texas) **Storm causes 200,000 outages at Oncor.** Storms across Texas caused more than 200,000 Oncor customers to lose electricity Thursday. Oncor said in addition to 2,000 of its employees, the company has enlisted more than 2,000 outside contractors to help restore power. In the Dallas-Fort Worth area, about 175,000 homes and businesses were without power by midday Thursday. Six high-voltage lines serving the Irving, Mckinney, and Carrollton areas were on the ground or damaged. Power has been re-routed, but the lines will not be repaired for at least a week, Oncor said. "As the storm exits our system, we are experiencing more outages and discovering serious damage to critical equipment," Oncor's chief operating officer said. Oncor is also working to restore service to Breckenridge, where every major line into the city was either downed or damaged overnight. At the height of the

storm at 6 a.m., Oncor estimated roughly 250,000 outages overall.
Source: http://www.bizjournals.com/dallas/stories/2008/04/07/daily41.html

[Return to top]

Chemical Industry Sector

Nothing to Report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *April 11, Wall Street Journal* – (National) **Utilities fret as reactor-part suppliers shrink.** As utilities pursue a U.S. nuclear power revival, they are confronting worries that their dependence on a reduced number of suppliers, including many overseas, could result in shoddy or counterfeit parts being used in plants. On April 7, the U.S. Nuclear Regulatory Commission alerted utilities that it tackled two cases of suspected counterfeit parts at nuclear plants last year. The counterfeits did not result in any equipment failures or safety problems, the agency said. But it warned that vendors, "including foreign companies with little or no experience in the nuclear industry, have entered the market to supply parts and components."
Source:
http://online.wsj.com/article/SB120787585954606783.html?mod=googlenews_wsj
See also: http://www.ohsonline.com/articles/60718/

6. *April 11, Palm Beach Post* – (Florida) **Agency may fine FPL again.** The U.S. Nuclear Regulatory Commission (NRC) announced Thursday that its staff is recommending a $130,000 civil penalty against Florida Power & Light Co. (FPL) because an investigation found that Turkey Point security guards, all contractors with Wackenhut Corp., slept on the job. Six guards slept or served as lookouts for other guards who were sleeping "on multiple occasions" between 2004 and 2006, the NRC reported. In one case, in April 2006, a guard was "sleeping while on duty at a post in a vital area of the reactor," according to the NRC. The agency uncovered the violations during a 2006 investigation and revealed its findings in October. None of the six guards identified as sleeping or serving as lookouts remains at Turkey Point. FPL has 30 days to pay or contest the fine. The company plans to review the details of the findings, and then make a decision. Meanwhile, the NRC confirmed it was looking into security practices at FPL's other nuclear plant, on Hutchinson Island in St. Lucie County, where sources said several Wackenhut guards lost their jobs recently. "We do have a review of security issues at St. Lucie, but I can't comment any further," an NRC spokesman said Thursday.
Source:
http://www.palmbeachpost.com/business/content/business/epaper/2008/04/11/a1d_fplfine_0411.html

[Return to top]

Defense Industrial Base Sector

7. *April 11, Gizmodo.com* – (National) **New pictures of XOS Exoskeleton.** Popular Science has posted an article, including pictures and a video, on Sarcos-Raytheon's XOS Exoskeleton, a full-body motion-assisting suit that could soon be available to soldiers. When wearing XOS, one can lift a 200-pound weight and feel like it is just 20 pounds, or throw a punch and have the suit's metal fist follow through onto the target. The suit has an array of sensors that track the pilot's movements, echoing them with its hydraulic muscles at the same speed. Using XOS, the pilot can run, walk, cope with stairs and ramps, and lift heavy weights. It has been in development for a while and has one major hurdle to overcome: the tether. XOS can run off batteries, but only for 40 minutes. A director at the Natick Soldier Research, Development, and Engineering Center envisions the early version to be more of a workhorse than a warrior. A plugged-in suit, borrowing energy from a vehicle or a ship's generator, could help a soldier rapidly unload a helicopter stacked with heavy equipment or repair tanks with broken tracks. Although the Army hopes to begin field-testing this version of the XOS by 2009, Sarcos engineers are still working toward an entirely self-powered version. This summer, the company will launch a research program with an engine-design firm to develop a generator capable of powering the XOS for hours at a time.
   Source: http://gizmodo.com/378759/xos-exoskeleton-sends-sci+fi-shivers-down-our-spines
   See also: http://www.popsci.com/exoskeleton

8. *April 10, CNN* – (National) **Stolen military items for sale online.** Sensitive and stolen U.S. military items are being sold on eBay and Craigslist, according to a report by the Government Accountability Office (GAO). Government investigators posing as buyers were able to purchase a dozen prohibited military items on the popular online selling sites. The report notes that the items purchased could easily have been shipped overseas and "used directly against our troops and allies." The items include two F-14 fighter jet components, night vision goggles that allow the user to identify U.S. troops at night, Army combat uniforms, and special body armor vests. Most of the items bought were stolen from U.S. military facilities, the GAO said. Testifying before the House National Security and Foreign Affairs subcommittee Thursday, eBay's vice president said the company vigorously works to keep prohibited items off the site. "We created prohibited and restricted items policies and built tools using state-of-the-art technology to enforce those policies" he said. Craigslist says it uses similar measures and relies on users to police the site. Craigslist's chief executive officer told the subcommittee, "It would simplify things greatly if a law were passed banning the sale of any U.S. military item less than 50 years old."
   Source: http://www.cnn.com/2008/US/04/10/military.loot/index.html?eref=rss_tech

[Return to top]

Banking and Finance Sector

9. *April 11, USA Today* – (National) **Identity thieves tax the system.** Federal Trade

Commission complaints involving tax returns linked to identity theft rose to 20,782 in 2007, up 158 percent since 2003. Similar complaints to the IRS Taxpayer Advocate jumped to 3,327 in federal fiscal year 2007, up 644 percent in three years. The head of the IRS Taxpayer Advocate office reported to Congress early this year that identity theft has emerged as one of the top problems facing taxpayers. File with one stolen identity, claim multiple dependents and apply for the federal Earned Income Tax Credit, and an identity thief can snag a tax refund worth thousands of dollars, or more. "People create a phony business, phony children, phony working hours and other details to get a very nice refund," says an enrolled agent in Miami who says a client who ran an import-export business fell victim to just such a scheme. In an interview last week, the IRS deputy commissioner for services and enforcement said cracking down on identity theft and assisting its victims is now "a top priority here." The IRS recently established a Privacy, Information Protection and Data Security office to centralize the tax agency's handling of identity-theft issues and help provide assistance and consistent treatment to taxpayers whose personal information has been stolen. The IRS recently created an electronic marker to flag compromised Social Security numbers in a system that would alert employees agency-wide. The move is aimed at sparing identity-theft victims from having to prove their claim year after year.
Source: http://www.usatoday.com/money/perfi/taxes/2008-04-10-id-theft_N.htm

10. *April 11, USA Today* – (National) **Online crime's impact spreads.** There appears to be no end to the cybercrime wave despite daily headlines about the latest computer breach and the best efforts of hundreds of security companies. The latest estimate: $200 billion a year, rivaling the illicit markets for drug trafficking and money laundering, says a chief research officer at computer-security firm F-Secure. He was among scores of computer-security experts here this week to discuss how data theft and Internet-enabled financial fraud have evolved into a global enterprise as sophisticated and responsive to economic principles as any other industry. The hazards of surfing and shopping online have shaken consumer confidence in e-commerce. Nearly 60 percent of Americans are fearful someone will steal their account passwords when they bank online, and 38 percent do not trust making payments online, according to a survey of 1,000 U.S. adults conducted by TNS Sofres on behalf of digital-security company Gemalto. Bank accounts were the most commonly advertised item for sale on underground computer servers, accounting for 22 percent of all items in the last six months of 2007, according to a Symantec report this week. Botnets are also increasingly spreading at financial institutions. The top botnets send a staggering 100 billion spam e-mail messages each day, SecureWorks says.
Source: http://www.usatoday.com/tech/news/computersecurity/2008-04-10-cybercrime-computer-security_N.htm

[Return to top]

Transportation Sector

11. *April 11, NY Times* – (National) **Southwest planes had cracks an inspection might have found.** Five Southwest Airlines planes grounded last month because they had not been properly inspected had precisely the kind of cracks that the inspection order was

intended to detect, an official of the agency testified Thursday to a Senate subcommittee. The testimony, by the associate administrator for safety of the Federal Aviation Administration, was the most explicit statement so far that the epidemic of aircraft groundings had genuine safety roots. In recent audits to determine if the airlines were complying with FAA orders, "we found we had achieved 99 percent compliance, but it's the other 1 percent that keeps me up at night," said the FAA associate administrator. He used stronger language to describe what Southwest had done in flying planes that it knew had not been properly inspected. While the airline's executives testified under oath last week that there was no safety-of-flight problem, the FAA official's prepared testimony said the flights had been putting thousands of passengers at risk. Some senators said, however, that in a data-driven system, under which FAA inspectors mostly review records rather than look at aircraft, the agency might have lost touch with actual conditions. In addition to the current maintenance crisis, the agency faces severe challenges in hiring employees in large numbers to replace air traffic controllers and safety inspectors; thousands have reached retirement age in the last few years or will soon.
Source:
http://www.nytimes.com/2008/04/11/business/11plane.html?ex=1365652800&en=8df9b2c879efdfbc&ei=5088&partner=rssnyt&emc=rss

12. *April 11, Florida Times-Union* – (Florida) **Underwater eyes in 3-D to secure port.** Jacksonville, Florida police assigned to secure the Port of Jacksonville have purchased Coda Octopus Group's Underwater Inspection System, cutting-edge sonar equipment that is expected to keep ships safe and curtail dangerous diving missions in the St. Johns River. Jacksonville Sheriff's Office is the first local law enforcement agency in the nation to use the equipment. Port authority officials have welcomed the extra security. In 2007, nearly 130,000 people boarded cruise ships at the port, while 8.3 million tons of cargo were loaded and off-loaded at the docks. Container traffic is expected to double after the TraPac terminal, scheduled to open within the next year at Dames Point, hits capacity.
Source: http://www.jacksonville.com/tu-online/stories/041108/bus_267298006.shtml

13. *April 10, Los Angeles Times* – (California) **Suspicious package shuts 241 tollway.** A suspicious package shut down traffic on the 241 toll road for more than two hours Wednesday afternoon before the object was removed by the Orange County, California Sheriff's Department bomb squad. The trouble began about 3 p.m., when a passerby told authorities that a box had been placed next to an emergency call box on the tollway near the 91 Freeway, according to the California Highway Patrol. CHP officers went to the scene and called in the sheriff's bomb squad after finding that the box was labeled "Explosive Device," authorities said. Bomb experts sent in a robot to pick up the package and drop it into a protective case. The ramp for the westbound 91 was shut down, snarling traffic on the tollway for about five miles before the road was reopened at 5:30 p.m. An Orange County sheriff's spokesperson said the box contained an artillery simulator -- a type of pyrotechnic device that causes a large flash, a boom and a cloud of smoke when ignited.
Source: http://www.latimes.com/news/local/la-mew-tollway10apr10,1,677322.story

14. *April 10, Reuters* – (National) **American Airlines cancels 570 Friday flights.** American Airlines said on Thursday that it has canceled around 570 flights scheduled for Friday as it works to complete the inspections of its MD-80 fleet as required by the Federal Aviation Administration.
Source: http://www.reuters.com/article/domesticNews/idUSN0946468120080410?feedType=RSS&feedName=domesticNews

[Return to top]

Postal and Shipping Sector

Nothing to Report

[Return to top]

Agriculture and Food Sector

15. *April 11, WebMD* – (National) **CDC: U.S. food safety hasn't improved**. The Centers for Disease Control and Preventions's Foodborne Diseases Active Surveillance Network, called FoodNet, began tracking cases of food-borne illnesses in 1996 in 10 U.S. states. The idea is to track infection trends for the 10 most important causes of food poisoning. "There is not a particularly important change from the last few years," said the deputy director of the CDC's division of food-borne diseases. "A lot of things have been going on to improve food safety, and we think they are likely to bear fruit ... but we cannot say we have made tremendous progress in the last year." While there have been significant declines in food-borne illnesses since 1996, there has been no significant improvement since 2004. Compared with 2004-2006, there has been no real decline in cases of food-borne disease caused by campylobacter, listeria, salmonella, shigella, E. coli, vibrio, or yersinia bacteria. 2007 was also a year in which there were several widespread outbreaks of salmonella infection, including outbreaks from contaminated peanut butter, frozen pot pies, vegetable snacks, and live pet turtles.
Source: http://www.cbsnews.com/stories/2008/04/10/health/webmd/main4007944.shtml

16. *April 11, Associated Press* – (National) **Dangerous animal virus on US mainland?** Concerns are being raised over an effort to move research on foot and mouth disease from an isolated island laboratory to the U.S. mainland near herds of livestock. Skeptical congressmen are demanding to see internal documents they believe highlight the risks and consequences of the decision. An epidemic of the disease could devastate the livestock industry. One such government report, produced last year and already turned over to lawmakers by the Homeland Security Department, combined commercial satellite images and federal farm data to show the proximity to livestock herds of locations that have been considered for the new lab. Sites in Georgia, Kansas, North Carolina, Texas, and Mississippi are being considered for the new lab, which would open in 2014. The existing lab in New York's Long Island Sound is accessible only by ferry or helicopter. However, there are financial concerns about operating from a

location with such limited access. The Homeland Security Department is convinced it can safely operate the lab on the mainland, saying containment procedures at high-security labs have improved, however the livestock industry is divided.
Source: http://www.foxnews.com/story/0,2933,350135,00.html

17. *April 11, Los Angeles Times* – (National) **USDA scientists say irradiation could be key to food safety**. Before bagged leafy greens are served, they are washed, often three times, in a potent chlorine bath. But new research shows the steps that California companies rely on to protect consumers do not kill dangerous bacteria inside the leaves, whereas zapping them with radiation does. The debate over how to protect consumers from E. coli and other potentially deadly microbes has intensified since the fall of 2006, when at least 200 people across the nation became ill and three died after eating tainted spinach. Irradiation, which involves bombarding food with high-energy gamma or electron beams to disrupt the DNA of pathogens, has its supporters and critics. But the new research suggests that it may be the only way to penetrate leafy greens and kill bacteria hiding inside. Although some hamburger meat, poultry, and spices are irradiated to kill bacteria, its use on fruits and vegetables to enhance food safety is not permitted in the U.S. Some produce is irradiated for insect control and shelf-life extension. The Food and Drug Administration is considering whether to allow the practice for killing pathogens, which would make it much more widespread. No health problems have been associated with eating irradiated food, but some consumer groups say its safety is unproven and have raised concerns about radioactive waste and accidental radiation releases.
Source: http://www.latimes.com/features/health/medicine/la-na-greens11apr11,1,1688105.story

18. *April 10, Associated Press* – (California) **Slaughterhouse gets $67M recall bill.** The U.S. Department of Agriculture said Thursday it has billed Westland/Hallmark Co. $67.2 million for more than 50 million pounds of beef the government purchased for the National School Lunch Program. The beef was part of the largest beef recall in U.S. history. The Department of Agriculture recalled 143 million pounds of beef in February after the Humane Society of the United States released undercover video showing plant employees abusing sick or weakened cows at the company's slaughterhouse. An agency review found that some of the so-called "downer" cows were slaughtered in violation of USDA policy, which prompted the recall. Further bills for the cost of destroying the beef and resupplying affected schools could cost up to $50 million more, the USDA's Agricultural Marketing Service said.
Source: http://ap.google.com/article/ALeqM5ib5V7z9A-ocCTOvoaRCq9Ohbl9SAD8VV63M00

[Return to top]

Water Sector

19. *April 10, Associated Press* – (Colorado) **Tests find Alamosa water had parasites as well as salmonella.** New test results show the tap water in Alamosa, Colorado, was tainted with two parasites as well as salmonella, but a chlorine flush of the system

probably killed all three types of contamination, officials said this week. Tests completed Wednesday on water samples taken before the chlorine flush began found traces of the giardia and cryptosporidium parasites, state health officials said. Further tests are planned, but officials have said residents of this southern Colorado city of 8,500 could be able to drink tap water again on Saturday for the first time in nearly three weeks. It was unclear how long the parasites had been in the water, but they have not been linked to any reported illnesses. Officials are unsure how salmonella got into the water but say a cracked pipe could be to blame.
Source: http://www.summitdaily.com/article/20080410/NEWS/548462566

20. *April 10, KYTV 3 Springfield* – (Arkansas) **Water main break adds to high water woes in Searcy County, Ark.** Rushing water in Searcy County, Arkansas, washed out an eight-inch water main that serves about 1,300 people. It was washed out along with the road. "If we don't get this fixed, the tanks will run dry," said the mayor of Marshall. Crews were still working on it on Thursday evening. "This is the only water source so we'll try to get it fixed first," said the mayor. The National Guard and the Arkansas Department of Emergency Management brought in bottled water for the 1,300 people served by the water main.
Source: http://www.ky3.com/news/local/17496379.html

21. *April 10, Associated Press* – (Alabama) **Alabama Legislature votes for water management committee.** The Alabama Legislature passed a resolution Thursday to develop a statewide water management plan, which, despite a severe drought and years of tri-state water talks, the state does not have. The resolution, if signed by the governor, will create the Alabama Permanent Joint Legislative Committee on Water Policy and Management. A supporter of the bill said Alabama has been criticized in its water-sharing talks with Georgia and Florida for not having a statewide water management plan. The resolution will correct that shortcoming, she said. The governor, who is in China on a trade mission, will review the resolution when he returns and decide whether to sign it, his press secretary said. Another supporter of the bill said the severe drought Alabama experienced last year showed the need for a water management plan. He said Alabama knows lots about its rivers and other surface water, but not enough about how much water is under the ground. Determining that will be a key step in developing a management plan. The committee will be made up of 14 legislators and will have several advisory members, including the state agriculture commissioner, state geologist, and director of the state environmental agency. The committee, which will operate permanently, will make a continuous study of the state water supply and its future needs and availability of water. It will develop conservation programs and make annual reports to the Legislature.
Source: http://www.al.com/newsflash/regional/index.ssf?/base/news-35/120785875549430.xml&storylist=alabamanews

22. *April 10, WXIA 11 Atlanta* – (Georgia) **How much water is Atlanta losing?** In a recent article, Popular Mechanics magazine ranked Atlanta's water system as one of the worst infrastructure projects in the U.S. Officials say that every day, what amounts to 17 million gallons of water is wasted or "unaccounted for." The city says it is repairing 800

leaks a month, to stop even more water from going to waste. Popular Mechanics said that despite the drought, 18 percent of the city's water was "hemorrhaging" through leaking pipes. That assessment was in 2003. Now, Atlanta's watershed says 14 percent, or what amounts to nearly 17 million gallons of water a day, is unaccounted for. "And it's actually declining 1 percent a year because of all the work we're putting into the system," said a representative of Atlanta Watershed Management. It is wasted water that the representative says is comparable to other major cities that average ten percent, but the city is working to improve, as it undergoes a $3.9 billion overhaul of the aging water and sewer system.
Source: http://www.11alive.com/news/article_news.aspx?storyid=114283&provider=top

23. *April 9, Washington Technology* – (National) **Water, water, everywhere under attack.** Water utilities should begin work immediately to secure their systems against catastrophic cyberattack, according to a new strategy document sponsored by the American Water Works Association and Homeland Security Department. The cyberthreat to water systems is growing, the report said. For example, in St. Louis in 2005, cyberattacks on gauges at the Sauk Water Storage Dam resulted in an unauthorized release of a billion gallons of water. In Harrisburg, Pennsylvania, in 2006, a hacker planted malicious software in a filtration plant that could have affected water treatment operations. The Roadmap to Secure Control Systems in the Water Sector outlines one-year, three-year, and ten-year goals for water utilities to upgrade their control systems and information technology architectures and networks to protect against cyberattacks and identify vulnerabilities. Within a year, water plants ought to create teams of IT and control engineers, integrate control system security needs into vendor contracts, and elevate control system security in all business plans, the report indicated. Within ten years, the water systems ought to have a robust portfolio of security tools and systems along with new IT architectures, protection for older systems, and secure communications. Water utilities are facing many challenges in implementing the road map at a time when cyberthreats are increasing, the report said. Foremost among them is that managers of such utilities often do not recognize the significance of the cyberthreat against industrial control systems.
Source: http://www.washingtontechnology.com/online/1_1/32592-1.html

[Return to top]

Public Health and Healthcare Sector

24. *April 11, Daily News* – (Massachusetts; New Hampshire) **Lyme disease makes heavy push over N.H. border.** Northeastern Massachusetts has long been plagued by Lyme disease-carrying ticks, but a recent study in Southern New Hampshire shows the problem is spreading rapidly over the state border. The New Hampshire Department of Health and Human Services released data this week that indicated more than 50 percent of ticks tested last fall in Rockingham County were carriers of Lyme disease. That is almost twice as many as experts had initially predicted. Since 2004, the number of confirmed cases of humans contracting Lyme disease in Rockingham County had nearly quadrupled, from 103 in 2004 to 389 last year. While the disease can be treated with antibiotics, it also can lead to serious illness or death if not diagnosed and treated

quickly. “(Massachusetts is the) ideal habitat for Lyme disease,” the medical director of the epidemiology program for the Massachusetts State Health Department said. “The missing piece has tended to be deer. The deer are returning to lots of communities where they haven’t been in a while.”
Source: http://www.newburyportnews.com/punews/local_story_102060858.html

25. *April 10, Reuters* – (National) **Genzyme recalls three transplant drug lots-US FDA.** Genzyme Corp. has voluntarily recalled three lots of Thymoglobulin, its injectable drug for transplant patients, after one lot failed a stability test, the U.S. Food and Drug Administration said on Thursday. The FDA, in a notice dated April 9, but released on Thursday, said one lot did not meet appearance requirements and the other two lots were predicted to have the same problem. The drug, used to treat acute rejection in organ transplant recipients, is supposed to appear clear to milky when reconstituted, but recent tests showed it was too cloudy in appearance, the FDA said.
Source: http://www.reuters.com/article/rbssHealthcareNews/idUSN1032669520080410

26. *April 10, Reuters* – (National) **U.S. reviews rare disorder with Roche, Novartis drugs.** Genzyme U.S. health regulators are investigating whether two transplant drugs made by Roche Holding AG and Novartis AG could be linked to a rare central nervous system disorder, the U.S. Food and Drug Administration said on Thursday. The two drugs, Roche’s CellCept and Novartis’ Myfortic, are used to prevent organ rejection. The FDA said it is reviewing whether they may trigger a potentially fatal disease called progressive multifocal leukoencephalopathy, or PML. The FDA said Roche is aware of patients who have developed PML, and the company has given the agency related information as well as proposed updating prescribing information for the drug. The FDA said it has also asked Novartis for related data.
Source:
http://www.reuters.com/article/governmentFilingsNews/idUSWBT00874420080410

27. *April 10, Times of India* – (International) **Bird flu virus may have got entrenched in India.** On April 10, the United Nations said that the highly pathogenic H5N1 avian influenza virus might now be entrenched in the Indo-Gangetic plains of India and Bangladesh. This is evidenced by the spread of the disease from West Bengal into Tripura, where the disease has killed approximately 3000 birds, forcing the state government to implement steps to deal with crisis. Culling operations began in a number of villages there after Tripura’s secretary of Union Animal Husbandry confirmed the outbreak.
Source: http://timesofindia.indiatimes.com/rssarticleshow/msid-2939607,prtpage-1.cms

Government Facilities Sector

Nothing to Report

[Return to top]

Emergency Services Sector

28. *April 10, DHS Press Release* – (National) **DHS-FEMA releases preliminary observations from national exercise TOPOFF 4.** "The U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) met today with State Homeland Security Advisors, State Emergency Management Directors and participants from the TOP OFFICIALS 4 (TOPOFF 4) exercise held in October 2007 to discuss preliminary exercise observations. During the meeting, held in Oklahoma City at the Memorial Institute for the Prevention of Terrorism (MIPT), officials briefed out and released preliminary exercise observations and lessons learned from TOPOFF 4. At the conclusion of TOPOFF 4, participants in the full scale exercise presented their initial impressions and identified major findings during a series of "hot-wash" briefings. The results of the briefings combined with an initial analysis of exercise play and inputs from participating departments and agencies were compiled into the official TOPOFF 4 Quick Look Report (QLR). The QLR summarizes the initial findings from the TOPOFF 4 exercise for the general public while providing stakeholders with the necessary material to begin a more detailed and comprehensive after action review process. The QLR focuses on five DHS capabilities, including: Intelligence/Information; On-Site Incident Management; Emergency Operations Center Management; Emergency Public Information and Warning; and Economic and Community Recovery. The Quick Look Report can be found at www.fema.gov.
Source: http://www.fema.gov/news/newsrelease.fema?id=43170

[Return to top]

Information Technology

29. *April 11, IDG News Service* – (National) **Oracle to ship critical database fixes next week.** Oracle Corp. plans to release patches for a slew of products next week, including fixes for two vulnerabilities in its database software. In total, Oracle plans to release 41 bug fixes Tuesday, but users are likely to pay particular attention to two bugs in the database that can be exploited over a network without a username and password. Oracle plans to ship 17 database fixes in all. News of next week's patches was announced Thursday on the company's Web site. More details will be released on Tuesday, but Oracle said that Versions 9i, 10g and 11g of its database are affected. The next most-patched product will be Oracle's E-Business Suite, with 11 bug fixes affecting the Advance Pricing, Application Object Library, Applications Framework, Applications Manager and Applications Technology stack components. Three fixes each are expected for the company's Application Server and PeopleSoft products. The Siebel SimBuilder and Enterprise Manager software will also be patched next week, Oracle said.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9076958&taxonomyId=17&intsrc=kc_top

30. *April 10, Computerworld* – (National) **Attacks begin against critical Patch Tuesday bug.** Hackers are trying to exploit a critical Windows vulnerability just patched on

Tuesday, security researchers said this afternoon – and the only version of Windows not at risk is the unfinished Windows XP Service Pack 3 (SP3). Fortunately, attackers' incompetence means that these initial sorties have been unsuccessful, Symantec Corp. said in a brief warning to customers of its DeepSight threat service. "The DeepSight honeynet has observed in-the-wild exploit attempts targeting a GDI vulnerability patched by Microsoft on April 8, 2008," said Symantec in its alert. On Tuesday, Microsoft Corp. patched two bugs, both pegged as "critical," in Windows' GDI, or graphics device interface, one of the core components of the operating system. According to Microsoft, every current version of Windows, including the very newest, Vista SP1 and Server 2008, is open to attack. The vulnerabilities can be triggered by malformed WMF (Windows Metafile) or EMF (Enhanced Metafile) image files, Microsoft noted in its accompanying advisory. Analysts on Tuesday fingered the GDI bugs as the most dangerous of the 10 disclosed and patched by Microsoft that day. They noted similarities between the two new vulnerabilities and others revealed in late 2005, which were extensively exploited by attackers for months afterward.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9076800&taxonomyId=17&intsrc=kc_top

31. *April 10, Wired* – (International) **Espionage against pro-Tibet groups, others, spurred Microsoft patches.** Computer intruders targeting pro-Tibetan groups, U.S. defense contractors and government agencies slipped in through previously unknown security holes in Microsoft Office, prompting Microsoft to issue a flurry of patches to the software suite in 2006 and 2007, according to computer security experts. These attacks, which appeared to have originated in China, began in early 2006 when the attackers started sending e-mails to victims with booby-trapped Word documents and Excel spreadsheets attached. "We are seeing more and more spying done with Trojans, a shift that has happened in the last two years," the chief research officer for software security vendor F-Secure, told RSA conference attendees Thursday morning. The Pentagon and pro-Tibet groups have previously acknowledged the intrusions, but the researcher is the first to link the cyber espionage to a series of patches that Microsoft pushed out without explanation. Microsoft did not immediately reply to a request for comment. Another F-Secure researcher notes that from 2005 through early 2006, Microsoft issued few patches for its Office suite. But soon after there was an explosion of patches for critical bugs that could be used to infect a computer, including a record 26 patches in October, 2006, that fixed four critical bugs in Microsoft Office applications. Those fixes, he says, appeared contemporaneously with the rise of targeted attacks on defense companies, nonprofits and government agencies. "They now have an incentive to begin looking for bugs and exploiting them," he said. "Bad guys are finding these things fast."
Source: http://www.wired.com/politics/security/news/2008/04/chinese_hackers

32. *April 10, Network World* – (National) **Botnet economy runs wild.** Cybercriminals have created a global business with a supply chain every bit as organized and sophisticated as that of any legitimate business. The difference is that cybercrime takes advantage of unsuspecting consumers and insecure businesses to steal untold amounts of money.

According to security experts and spam fighters speaking at a panel discussion on Wednesday at the RSA Conference, the modern, online criminal ecosystem starts with botnets, which are consumer or college PCs that have been taken over by hackers. A cybercriminal can easily go online and buy a bot-herd. In fact, the manager of security programs at the Internet2 networking consortium and the University of Oregon said there are 5 million to 5.5 million botnets in active rotation at any time. Of course, cybercriminals need only a few hundred spambots to send out millions of spam e-mails. Today, a cybercriminal can hire programmers to come up with the latest and greatest types of spam, such as image spam or spam put into PDF attachments. Spammers send test runs through ISPs to see what types of spam get through the easiest, said Larry (who refused to disclose his last name) from the spam-fighting SpamHaus Project. The types of spam include the traditional "pump and dump" stock-manipulation spam, plus spam for a variety of products. Cybercriminals have become so good at it that they use phishing to fool customers into going to a fake pharmaceutical site and actually fulfill orders for drugs so they can get repeat business.
Source: http://www.networkworld.com/news/2008/041008-rsa-botnet-economy.html?fsrc=rss-security

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

33. *April 10, The Denver Post* – (Colorado) **DSL, wireless outage hangs up metro area.** A hardware failure resulted in the loss of broadband service for Qwest business and residential customers in the Denver area Thursday afternoon. A Qwest spokeswoman confirmed that the Denver-based phone and Internet service provider experienced "a hardware issue at its Denver main central office." "It affected broadband and data services. Services were out for approximately an hour," she said. "We're still evaluating the scope." She did not say exactly how many customers and businesses were affected by the outage, stating that the company was still evaluating the problem. Along Denver's 16th Street Mall, home to several office towers and workplaces for thousands, service was fine at Qwest's Solutions Center. The same could not be said for clients who came into the shop looking for answers. A customer-service representative contacted through Qwest's technical support number at 7 p.m. said the DSL outage was continuing in some places but that it did not affect analog lines. He said there was no estimated time when service would be restored but advised customers that service could be out for 24 to 48 hours. The spokeswoman said that time frame was "inaccurate." An AT&T spokeswoman said its wireless customers were affected because some cell sites are fed by Qwest switches. She said other wireless carriers also were hit.
Source: http://www.denverpost.com/business/ci_8885412

34. *April 10, Broadband Genie* – (International) **Fears for mobile broadband overload.** With the success of mobile broadband taking off faster than anyone could have expected, there are now concerns that European networks' ability to handle the new traffic has almost reached its capacity. Speaking on the subject, the CEO of 3 confirmed that there are now seven times more customers using mobile broadband since the introduction of the technology and reports suggest that networks are now preparing for this unexpected surge in mobile data usage. Before introducing data dongles to the UK, 3 tested out the technology in smaller European markets such as Sweden and Austria, and although the service seemed to work fine, it did not give enough indication of problems that could arise with the UK's higher demand. The CEO explained: "With mobile broadband, we have seen blockages in areas we didn't expect, but these have been easy to fix in the short term." He continued, "We had capacity issues in Sweden and Austria and they were harder to identify… Backhaul and capacity are relevant, and we need to have solutions in place. We are working on it already."
Source: http://www.broadbandgenie.co.uk/broadband-news/2008/04/11/fears-for-mobile-broadband-overload/

[Return to top]

Commercial Facilities Sector

Nothing to Report

[Return to top]

National Monuments & Icons Sector

35. *April 11, New York Times* – (National) **U.S., after a court reversal, issues new rules for forests.** The United States Forest Service has released new regulations for managing the country's 155 national forests, after a federal judge struck down an earlier set of rules. The service's associate chief said the rules, which took effect Wednesday, gave forest managers more power to react to natural disasters and climate change and to decide how land they supervise should be used. The new regulations also end the requirement that each species be evaluated for sustainability. Instead, the service will focus on the overall habitat in and around a national forest, it says. Environmental groups say the rules remove critical protections for wildlife and will allow more logging. At least one environmental law firm said it would challenge the rules.
Source: http://www.nytimes.com/2008/04/11/us/11forest.html?ref=us

[Return to top]

Dams Sector

36. *April 11, Daily Advertiser* – (Louisiana) **Corps to open Bonnet Carré Spillway for levee relief.** The U.S. Army Corps of Engineers is scheduled to start relieving pressure on Mississippi River levees today by opening some of the flood gates of the Bonnet

Carré Spillway at noon. Heavy rain in the Mississippi River Valley is prompting the opening for the first time in 11 years, although Corps officials say there is currently no danger of levees giving way or being overtopped. Without opening the gates to let some water escape into Lake Pontchartrain, the river flow at New Orleans would exceed 1.25 million cubic feet per second today, a Corps report says. Sand boils, where water comes under levees in sandy areas, are erupting in several areas all along the Mississippi, so crews are working to pack them with sand bags. The National Weather Service reported the river is at about 40.5 feet at Baton Rouge and is expected to crest at 42 feet April 21. "Flood stage without the levee is 35 feet," said a Coast Guard chief, so the river is considered at flood stage when it gets to that mark.
Source:
http://www.theadvertiser.com/apps/pbcs.dll/article?AID=/20080411/NEWS01/804110328/1002

37. *April 11, WSIL 3 Harrisburg* – (Illinois) **Help needed at the Brookport Levee.** Heavy rains from storms could cause flooding along the Ohio River near Brookport, Illinois. Already the town is using pumps to ease the pressure on its aging levee. Without constant eyes on these pumps, leaders say there could be several problems that would drive costs up even further. This is all in an effort to avoid flooding. The Brookport levee is old, and decades of wear are taking a toll. "The pipes that run through the levee are better than 60 years old and they rot out. That's our problem right now," a city councilman said.
Source: http://www.wsiltv.com/p/news_details.php?newsID=4589&type=top

38. *April 11, Oklahoman* – (Oklahoma) **Pond nears breaking point, flood warnings announced.** An Oklahoma City neighborhood was briefly in danger of flooding Thursday evening when a detention pond dam near Lake Hefner neared its breaking point, a city official said. The pond was about three feet above its safe level when emergency crews began work to drain it, said an assistant city engineer. By about 7:30 p.m., water pumps capable of removing 11,000 gallons of water per minute were in place. No evacuation was necessary, but residents were alerted to the possibility of flooding. A pipe underneath the dam became clogged sometime Thursday, which led to the dangerous water levels, the engineer said. Water eroded the area around a drain that feeds the pipe.
Source: http://newsok.com/article/3228492/1207890019

39. *April 11, Times Daily* – (Alabama) **Dam gets funds for repairs.** Sloss Lake dam in Alabama has received $300,000 in emergency funds to repair two large holes that threatened a potential dam collapse that would have affected at least 70 downstream residences. The grant money was awarded by the governor's office through the U.S. Department of Housing and Urban Development and will be administered through the Alabama Department of Economic and Community Affairs. "The threat posed by the possible breach of Sloss Lake dam requires timely action to avert a potential disaster," the governor said in a press release. "I commend city officials for alertly detecting and promptly responding to this threat to life and property." The leaks were found in early March and workers pumped out water from the 44-acre lake that holds more than 300

million gallons.
Source: http://www.timesdaily.com/article/20080411/NEWS/804110335/-1/COMMUNITIES02

[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) 312-5389
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 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