Department of Homeland Security
Daily Open Source Infrastructure Report for 9 April 2008

- According to Mercury News and the Associated Press, security has been beefed up at the Golden Gate Bridge and other well-known San Francisco landmarks in anticipation of Wednesday's Olympic torch relay and accompanying protests. San Francisco's mayor called on law enforcement and bridge officials to reassess their overall security strategy. (See item 12)
- The Times reports alarm about a flu pandemic has been restarted by clear evidence that bird flu can be transmitted person to person. A team of doctors led by a researcher from the Chinese Center for Disease Control and Prevention in Beijing reports that a man infected with the H5N1 virus passed the infection to his father, probably at the hospital. The two cases were detected in the family from Nanjing in December last year. (See item 22)

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 8, KONP AM 1450 Port Angeles* – (Washington) **Ecology plans San Juan oil spill strategy meetings.** The public is invited to help the state Department of Ecology and Coast Guard update and improve site-specific oil-spill response strategies used for the San Juan Islands, called geographic response plans. Ecology and the Coast Guard will hold two workshops this week – one in Friday Harbor and one in Eastsound –

where citizens, resource managers, spill response contractors, and oil-industry representatives can help identify any new information that might make the strategies more effective. Geographic response plans are oil-spill response strategies tailored to reduce the effects of oil spills to sensitive areas along beaches, shores, or waterways.
Source: http://www.konp.com/local/3527

[Return to top]

Chemical Industry Sector

2. *April 7, Houston Chronicle* – (National) **Senator asks agency for post-BP report.** A senator has asked the government agency that oversees worker safety to provide a detailed account of actions it has taken to address concerns raised by the deadly March 2005 explosion at BP's Texas City refinery. In a letter last week to the U.S. Occupational Safety and Health Administration, the Massachusetts representative asked the agency to provide details about refinery and chemical plant inspections and a nationwide audit program launched last year in response to refinery deaths, including those in Texas City. A Labor Department spokeswoman said OSHA had received the letter and is preparing a response. The official's letter said that the U.S. Chemical Safety and Hazard Investigation board concluded in its two-year investigation that OSHA contributed to the blast by failing to vigorously enforce its process-safety management standard at refineries and chemical plants. Process safety involves safe operation of equipment and handling of hazardous materials, as opposed to personal safety, or prevention of slips and falls. The chemical safety board's recommendations included that OSHA strengthen enforcement of process safety by identifying facilities at the greatest risk of catastrophe; conducting comprehensive inspections; and expanding process-safety training for inspectors.
Source: http://www.chron.com/disp/story.mpl/headline/biz/5682239.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *April 8, Brazosport Facts* – (Texas) **Nuke plant addresses staffing issues.** The South Texas Project is looking to education as it gears up to add 1,200 permanent employees by 2015 to address expected staffing needs. The South Texas Project is planning to build two reactors scheduled to come online by 2016. "We have a projection that over the next five to six years, we're going to add about 1,200 new workers here and that's to get ready for the two new units," said a South Texas Project spokesperson. The plant will need to hire people to work in areas such as, chemical, ratings and protection, electrical, mechanical maintenance, and other non-engineering skill sets, said the South Texas Project workforce development coordinator. The South Texas Project and the Mid-Coast Industry Education Alliance have developed a Nuclear Power Technology associate's degree to bring more people into the field, he said.
Source: http://thefacts.com/story.lasso?ewcd=81798378d799db8b

4. *April 8, Hartford Courant* – (Connecticut) **Millstone nuclear power plant incident**

investigated. The operator of the Millstone 2 nuclear power plant is investigating how 1,000 gallons of water from a reactor cooling system inadvertently leaked into a water storage tank Sunday, a mistake a company spokesman said has never before happened at the facility. No water was released into the environment, although the incident did cause a "minute amount" of radioactive gases to leak through an air vent in the storage tank, according to spokesmen for Dominion, the plant's owner, and the U.S. Nuclear Regulatory Commission (NRC). The release involved "extraordinarily low levels of radiation" far below the amount allowed under federal guidelines, an NRC spokesman said. The tank has an air vent, but the filter on the vent was not operating at the time of the incident, so some radioactive gases escaped. The water leak was detected about 12:30 p.m. as the reactor was being shut down for a scheduled maintenance and refueling. The leak reportedly was stopped within an hour. The director of the Connecticut Coalition Against Millstone said the tank's air vent lacked a radiation monitor and called the incident "greatly troubling." She called on the NRC to order Dominion to install such monitors on all potential radiation pathways.
Source: http://www.courant.com/news/local/hc-ctmillstone0408.artapr08,0,1850213.story?track=rss

5. *April 8, Louisville Courier-Journal* – (Kentucky) **Kentucky uranium waste could sell for $7.6B.** About 40,000 canisters of depleted uranium at the Paducah, Kentucky, Gaseous Diffusion Plant are getting a new look as a potential moneymaker for the federal government. In 2000, uranium sold for about $7 per pound. Today, the price is about $73 per pound. A congressman, in whose congressional district the Paducah plant is located, has introduced legislation directing the Department of Energy (DOE) to re-enrich the depleted uranium into usable fuel for nuclear reactors. The work would be done under contract with the United States Enrichment Corp. (USEC), which operates the Paducah plant. The assistant secretary for nuclear energy at the DOE told a House panel that his agency would require a cost-benefit analysis and environmental assessment before any reprocessing. Selling the depleted uranium on the open market could mean the material would end up being processed outside the U.S., warned the president of United Steelworkers Local 550, which represents 800 workers in Paducah. "We need to be promoting a viable and healthy domestic-enrichment industry," he said. The congressman said he plans to discuss with his colleagues the possibility of changing his bill to permit a combination of auctions and a reprocessing contract with USEC.
Source: http://www.usatoday.com/money/industries/energy/2008-04-07-uranium_N.htm?csp=15

[Return to top]

Defense Industrial Base Sector

6. *April 8, Washington Post* – (National) **U.S. weapons upgrade faces big hurdles.** The U.S. Army is in the early stages of developing the most expensive weapons program in its history – Future Combat Systems, a new generation of weapons, combat vehicles, robots, and sensors connected to a wireless network. The Army said the program will cost $162 billion including inflation. Independent estimates from the office of the Secretary of Defense price the project at $203 billion to $234 billion. The figures do not

take into account the expense of three complementary military programs – Joint Tactical Radio System, Warfighter Information Network-Tactical, and Transformational Satellite Communications (TSAT) – that are supposed to serve as a critical communications network for Future Combat Systems. The three projects are expected to be used by different parts of the military and cost about $80 billion combined. A Boeing executive said he expects the high-speed radios and the wireless network to be finished on time and to "dovetail very nicely with" Future Combat Systems. He said TSAT, a new constellation of satellites, is "not required." Other defense experts disagree, saying that the new, faster satellites are crucial to make Future Combat Systems work. Congressional investigators also question whether the complementary programs will be ready in time to be incorporated into the Army project, which also has been restructured in the face of immature technologies, rising costs, and timetable problems.
Source: http://www.msnbc.msn.com/id/24006579/

7. *April 2008, National Defense* – (National) **Navy may declassify its confidential wish-list.** The Navy's super-secret "strategic plan" can be described as the service's itemized wish-list that rarely anyone from the private sector gets to see. That may change in the future, suggested a recently retired commander of naval surface forces. The plan, which specifies what the Navy wants to buy to be able to execute its maritime strategy and concept of operations, is a classified document. In response to frequent complaints from industry, the Navy is considering releasing an unclassified version, he told an Armed Forces Communications and Electronics Association conference.
Source:
http://www.nationaldefensemagazine.org/issues/2008/April/WashPulse.htm#BigBucks

8. *April 2008, National Defense Magazine* – (National) **A makeover for top-heavy Navy ships?** Surface combatants that once carried only 40 to 75 antennas a decade ago are now sailing with as many as 150. "When you have lots of different apertures all around your topsides, you have issues of blockage, and you have issues of these antennas interfering with each other," says a deputy at the Office of Naval Research (ONR). Moreover, "whatever weight you add to the mast, you have to add to the keel for stability," says an ONR engineer. Such increases could translate into expanding the size of hulls, which raises costs. Scientists believe that they can help reduce those costs by miniaturizing many of the antennas' electronic components and by integrating them into more efficient, wideband arrays that will allow the various combats systems to share frequencies. The ONR engineer runs a program called aperstructures that seeks to eliminate antenna apertures on stick masts by incorporating the systems onto the sides of ships' deckhouses. By doing so, the superstructure itself becomes the aperture. Its larger size gives the antenna inherent power so that it does not have to rely as much on the ship's electricity to send and receive signals. Researchers will determine which systems pair together well and the optimum amount of frequency suitable for each array. Reducing the size, weight, and number of antennas will reduce the radar cross section of the topside and improve the vessel's survivability, says the engineer. Funding for the integrated topsides innovative naval prototype work commences next year.
Source: http://www.nationaldefensemagazine.org/issues/2008/April/InsideScience.htm

[Return to top]

Banking and Finance Sector

9. *April 8, Associated Press* – (National) **Online crooks face tough competition.** Fierce competition among identity thieves has driven the prices for stolen data down to bargain-basement levels, which has forced crooks to adopt mainstream business tactics to lure customers, according to a new report on Internet security threats. Data is usually sold through instant-message groups or Web forums that exist for only a few days or even hours, according to the latest twice-yearly Internet Security Threat Report from Symantec Corp. released Tuesday, and the hacking community exacts harsh consequences when members try to pass along fraudulent information. "If the seller says there's $10,000 in a bank account, and there isn't $10,000 in there, their ability to sell will drop through the floor," said the vice president of Symantec Security Response. Researchers said they found more evidence during the last six months of the year that Internet fraudsters are adopting mainstream tactics, including hiring teams of hackers to create new viruses and offering volume discounts on stolen data to encourage larger orders. In some cases, stolen credit card numbers were sold in batches of 500 for a total of $200. That is 40 cents each, less than half the price observed during the first half of 2007, when they were down to $1 apiece in batches of 100, according to the report. Full identities — including a functioning credit card number, Social Security number or equivalent and a person's name, address and date of birth — are going for as little as $100 for 50, or $2 apiece. Certain identities are more alluring than others, according the report. Stolen identities of citizens of the European Union sell on the high end — for $30 — an average of 50 percent more than U.S. identities. Researchers said the higher prices reflect the fact that the identities can be used in multiple countries, instead of just one. The survey is based on malicious code gathered from more than 120 million computers running Symantec antivirus software and some 2 million decoy e-mail accounts that collect spam.
   Source:
   http://news.yahoo.com/s/ap/20080408/ap_on_hi_te/internet_security_threats;_ylt=Avv0vTfJRkktSapUWIXxpN6s0NUE

10. *April 8, Associated Press* – (National) **Antioch University reports computer breach.** Antioch University says a computer system containing more than a decade of personal information on about 70,000 people was breached by a hacker. The university said there is no conclusive evidence that any personal information was stolen, but police are investigating. School officials last month recommended students, former students, applicants and employees monitor financial records and credit reports because of the breach. The system contains names, Social Security numbers, academic records and payroll documents for current and former students, applicants and employees going back to 1996. Antioch University also has campuses in New Hampshire, Ohio, Washington State and California.
    Source: http://www.wcsh6.com/news/article.aspx?storyid=84339

11. *April 7, Washington Post* – (National) **RedBox warns of credit card skimmers.** DVD-rental vending machine maker RedBox warned customers to be on the lookout for any unusual activity or physical changes to local RedBox kiosks, after the company

discovered evidence that criminals had retrofitted at least three of the machines with devices to steal credit-card information. The company said several RedBox machines had been fitted with “skimmers” -- magnetic stripe reading and storage devices that can be installed over the top of existing card readers. RedBox said it found an illegal skimming device attached to one machine in Tempe, Arizona, and that it had discovered evidence of skimming at two other locations in Las Cruces, New Mexico. In a notice posted on its Web site, Redbox said is not aware of any fraudulent activity or transactions using its customers’ accounts, and that it is working to minimize the risk of this happening. But the company is urging customers to be vigilant for signs of tampering at any of its 7,400 Redbox locations nationwide.
Source:
http://blog.washingtonpost.com/securityfix/2008/04/redbox_warns_of_credit_card_sk.html

[Return to top]

Transportation Sector

12. *April 8, Mercury News & Associated Press* – (California) **Breach of Golden Gate Bridge security rattles S.F. officials.** Monday’s daring Golden Gate Bridge protest of the Olympic torch relay has San Francisco officials vowing to put security first, even if it could mean further shortening or last-minute changes to Wednesday’s six-mile relay route. Already, all vacations have been canceled for San Francisco police officers and security has been beefed up at the Golden Gate Bridge and other well-known city landmarks in anticipation of the relay and counter-protests. The bridge’s sidewalks were closed, and will be through the relay event. San Francisco’s mayor, on Monday, also expressed concern about how the protesters could so easily scale the bridge’s suspension cables in the wake of tightened security since the September 11, 2001, terrorist attacks. He called on law enforcement and bridge officials to reassess their overall security strategy. For nearly three hours Monday, three pro-Tibet activists dangled at least 150 feet above the bridge, drawing international attention, slowing traffic and marking the start of what anti-Chinese groups promise will be several days of Bay Area protests accompanying Tuesday’s arrival of the Olympic torch and Wednesday relay along the city’s Embarcadero.
Sources:
http://www.mercurynews.com/othersports/ci_8848628?nclick_check=1&forced=true

13. *April 7, KNTV 11 San Jose* – (California) **FAA implements airspace restrictions over Olympic torch route.** The Federal Aviation Administration announced Monday that it will implement airspace restrictions around the Beijing Olympic torch relay route in San Francisco Wednesday, creating space for the high number of law enforcement helicopters that will hover above the event. The restrictions, which will be in effect between 12:30 p.m. and 5 p.m., will apply to airspace from ground level to 3,000 feet in areas around the route, according to a FAA spokesman. Law enforcement, media, and emergency aircrafts will be allowed to fly in the restricted zone but must maintain contact with air traffic controllers at all times, he reported. Private pilots will not be allowed to enter the restricted zone. The restrictions will be lifted when the relay ends,

according to the same official.
Source: http://www.nbc11.com/newsarchive/15818263/detail.html

14. *April 7, Business Week* – (National) **FAA proposal would help avoid flameouts.** The Federal Aviation Administration on Monday proposed new safety procedures to ensure that jet engines do not stop in midair during icy weather. The FAA said it had received reports indicating a dozen or more instances in which one or more engines aboard airliners shut down in ice-crystal conditions during descent, an event referred to as engine flameout. In all cases, crews were able to restart the engines. Under the proposed rule, before beginning a descent pilots would activate anti-ice systems aboard aircraft more frequently in extreme weather conditions involving ice crystals. The regulatory agency said there were reports of six engine flameouts on McDonnell Douglas Model MD-11 airplanes; several such events on Boeing Model 767 airplanes and four on Model 747 planes. "These are rare events and engine reliability is high now, but our aim is to give pilots the help they need to avoid even the rare instances when a problem might occur," said an FAA spokeswoman.
Source: http://www.businessweek.com/ap/financialnews/D8VT7BL01.htm

[Return to top]

Postal and Shipping Sector

Nothing to Report

[Return to top]

Agriculture and Food Sector

15. *April 8, Associated Press* – (National) **Great Lakes shippers take steps to halt deadly fish virus spread.** Great Lakes shippers say they are taking steps to keep a deadly fish virus from spreading into Lake Superior through ballast water. The Lake Carriers' Association said Monday the measures will reduce the threat of viral hemorrhagic septicemia entering the lake or spreading there. The virus has been found in the other Great Lakes and in some inland lakes. The group says freighters will try to take on ballast water in deep water away from shore and will re-circulate ballast water in their tanks to chop up any fish it may contain. A Wisconsin state fisheries official says the measures may help, but ballast water could still contribute to the spread of disease and exotic species.
Source:
http://www.mlive.com/environment/index.ssf/2008/04/great_lakes_shippers_take_step.html

16. *April 7, Reuters* – (National) **Boston Beer recalls select bottles of Samuel Adams beer.** Boston Beer Company Inc. recalled select bottles of its flagship Samuel Adams beer after safety checks at its Cincinnati brewery stoked fears that bottles may contain small grains or bits of glass. The routine quality-control checks of its 12 ounce glass beer bottles, manufactured by a third-party glass bottle supplier, detected defects that

might cause small bits of glass to break off and possibly fall into the bottle, Boston Beer said in a statement. Boston Beer said it has had no reports of any consumer injury, but the presence of small bits of glass in the bottle could pose a health risk "under certain circumstances." The defective bottles come from a plant that supplies about 25 percent of the company's bottles. The number of bottles that contain glass pieces is less than one percent of the total number of bottles supplied from the plant, the company said.
Source:
http://news.yahoo.com/s/nm/20080407/bs_nm/bostonbeer_recall_dc;_ylt=AidITySx3EexJztYTTpDuzMWIr0F

17. *April 7, Chicago Sun-Times* – (National) **Jewel-Osco stores recall contaminated cereals.** Jewel-Osco stores are temporarily recalling their brand of cereals after the Minneapolis-based company Malt-O-Meal found Salmonella contamination in its product. On Friday, Malt-O-Meal announced a voluntary recall of their unsweetened Puffed Rice and unsweetened Puffed Wheat Cereals with "Best If Used By" dates between April 8, 2008 and March 18, 2009, according to a company release. Malt-O-Meal distributes cereal nationally and produces "private label brands" such as America's Choice, Jewel, ShopRite, Tops, Weis Quality, Pathmark, Laura Lynn, Food Club, Giant, Acme, and Hannaford, the release said. In Illinois, Indiana, and Iowa, Jewel Puffed Rice and Jewel Puffed Wheat cereals have been recalled by the company.
Source: http://www.suntimes.com/news/metro/882062,recall040708.article.

18. *April 7, Reuters* – (National) **No quick end for cloning product moratorium: USDA.** The U.S. Agriculture Department said on Monday it will not lift a voluntary moratorium on selling meat and milk from cloned animals to consumers any time soon. In January, the U.S. Food and Drug Administration ruled that products from cloned cattle, swine, goats, and their offspring were as safe as milk and meat from traditional animals. Before then, farmers and ranchers had followed a voluntary ban on the sale of cloned products. After the FDA's ruling, USDA asked the industry to prolong the ban for a transitional period expected to last several months. USDA is now responding to questions and concerns in the sector and working with other countries reviewing cloned products. Even after the ban is lifted, it could take three to five years before consumers are able to buy clone-derived food as animals need to be cloned, and then mature and give birth. Milk and meat would come from the offspring of cloned animals, which the industry and FDA view like any other offspring from traditional animals. Currently, an estimated 600 cloned animals exist in the U.S. So far, major food companies including Tyson Foods Inc. and Smithfield Foods Inc. have said they would avoid using cloned animals.
Source:
http://www.reuters.com/article/scienceNews/idUSN0438308520080407?sp=true

19. *April 7, KXRM 21 Colorado Springs* – (Colorado) **Public health is at a "breaking point".** El Paso County departments are struggling with serious cutbacks and the possibility of more in the future. Officials from the Health Department spoke out at a forum on the county budget crisis Monday. The forum came on the heels of the salmonella outbreak in Alamosa. El Paso County's commissioner said: "As the budget gets tighter, our ability to react is much slower." The health department said the number

of restaurant-related complaints and violations increased six-fold, but the number of inspectors has declined, adding that they do not have the resources to protect the community from the threats of illness. Elected officials said the community must understand the health department is at a "breaking point."
Source: http://fox21news.com/news/news_story.aspx?id=118249

[Return to top]

Water Sector

20. *April 7, WKMG 6 Orlando* – (Florida) **Town considers forcing 100-gallon-per-person water limit.** A small town in central Florida is considering forcing a 100-gallon-per-person daily limit on water for its residents. Some residents in Oakland, which is located south of Apopka, are outraged over the proposed limit on water and said the rapid growth in the area must stop until there is no longer a shortage. The proposal comes days after the Orange County mayor said that if the county does not have a 40 percent reduction in water use, the aquifer will not have enough water to sustain the county. Similar to surrounding cities, water bills in Oakland order "no watering on any day between 10 a.m. and 4 p.m. or face a $500 fine." Local 6 reported that an average resident can use up to 90 gallons of water before leaving the house for the day. Commissioners are proposing a 500,000 gallon water tank, Local 6 has learned.
Source: http://www.local6.com/news/15811993/detail.html

[Return to top]

Public Health and Healthcare Sector

21. *April 8, Xinhua* – (International) **Four cases of outbreaks of influenza-like illness reported in HK.** Hong Kong's Center for Health Protection (CHP) of the Department of Health received four reports of outbreaks of influenza-like illness on Tuesday, said a government press release. According to the press release from the Information Services Department of Hong Kong Special Administrative Region government, the four cases involve three primary schools and one kindergarten/child care center, affecting a total of 18 students. A CHP spokesman said that influenza-like illness may be caused by influenza or other respiratory viruses. CHP's officials have visited all the institutions and provided health advice to the staff accordingly. No report was received on Tuesday under the influenza surveillance arrangement set up by CHP with private and public hospitals. The spokesman urged members of the public to stay alert by taking precautionary measures against influenza. On the night of March 12, Hong Kong government announced the closure of all primary schools, special schools, and kindergartens in the city for two weeks due to seasonal flu outbreaks.
Source: http://news.xinhuanet.com/english/2008-04/08/content_7941316.htm

22. *April 8, Times* – (International) **Bird flu: father infected by dying son.** Alarm about a flu pandemic has been restarted by clear evidence that bird flu can be transmitted person to person. This could be one of the first steps in the evolution of the H5N1 strain of avian flu into a deadly pandemic strain that could infect hundreds of millions of people.

The new evidence involves a 52-year-old man who caught the disease from his 24-year-old son, who himself seems to have contracted it up at a poultry market. The son died, while his father narrowly survived. A team of doctors led by a researcher from the Chinese Center for Disease Control and Prevention in Beijing, report in the Lancet online that the two cases of avian flu were detected in the family from Nanjing in December last year. Just before the man died, tests showed that he was infected by H5N1 avian flu virus. His father, a retired engineer, lived six miles away. When his son fell ill he went to see him and helped to look after him in hospital for two days. The father fell ill a week later, but survived after being treated with antiviral drugs and blood plasma from a woman who had been deliberately infected with inactive H5N1 in a clinical trial. Samples of H5N1 virus taken from the father and son were genetically identical, save for one small change. The flu virus mutates rapidly, so the fact that these two samples were so nearly identical is strong evidence of direct human infection . Sourcehttp://www.timesonline.co.uk/tol/life_and_style/health/article3701724.ece

23. *April 7, Desert Sun* – (California) **West Nile Virus detected in east valley, fogging taking place.** In California, the Coachella Valley Mosquito and Vector Control District is conducting aerial and ground fogging in the east Coachella Valley after workers found West Nile virus in four mosquito pools. Fogging will take place in the area southeast of Mecca and near North Shore through the middle of next week, according to the district. West Nile has never been detected in the North Shore and fogging is being done there as a precaution.
Source:
http://www.mydesert.com/apps/pbcs.dll/article?AID=/20080407/NEWS07/80407036/1263/UPDATE

Government Facilities Sector

24. *April 8, Associated Press* – (Florida) **Lab tests to determine what closed Orange County Sheriff's Office.** Orange County, Florida, authorities are waiting for lab results to determine what was in a package that forced the evacuation of the sheriff's office headquarters. The Orlando building was evacuated Monday morning. A sheriff's spokeswoman said then that two employees had burning and watery eyes after coming into contact with the package. They were treated at the scene. Technicians took samples of the package for testing. More than 600 employees were evacuated at the time. Authorities say the package was found to be free of any hazardous materials, devices, or dangerous substances. The air conditioning system also was checked for any problems. Authorities are tracking down who delivered the package on Friday.
Source: http://www.mysuncoast.com/Global/story.asp?S=8134119&nav=menu577_2_1

25. *April 7, Associated Press* – (National) **Report: IRS computers vulnerable to hackers.** A week before the tax filing deadline, Treasury Department watchdogs say that inadequate controls over the IRS computer system could make confidential taxpayer information more vulnerable to hacking and theft. The office of the Treasury Inspector General for Tax Administration is warning that the lack of monitoring could allow a

disgruntled employee or a hacker to disrupt computer operations and steal taxpayer data. The IRS agreed that it needs to improve oversight of who has access to its computers.
Source: http://www.foxnews.com/story/0,2933,347488,00.html

[Return to top]

Emergency Services Sector

26. *April 8, Occupational Health & Safety* – (National) **UP-Dow chemical safety train ready to roll.** A safety train fitted with a classroom and training center will visit 10 communities along the Mississippi River corridor during the next month to provide free railroad and chemical transportation training to local firefighters and emergency responders. The 2008 TRANSCAER (Transportation Community Awareness and Emergency Response) Training Tour, presented by Union Pacific Railroad and Dow Chemical Co., begins April 9 in Alexandria, Louisana and ends May 8 in Chicago. TRANSCAER is a voluntary national outreach consortium of chemical-related companies, transport companies, and associations created 22 years ago. It "is an important extension of our industries' shared commitment to the security and safety of the many people and communities we touch," said a Dow's Emergency Services and Security representative. "This program and the resources it makes available are intended to help safeguard the public by providing first responders with the information and training they need to effectively respond in the unlikely event of a chemical transportation incident."
Source: http://www.ohsonline.com/articles/60548/

27. *April 7, Muskogee Phoenix* – (Oklahoma; Arkansas; Texas; Mississippi) **Mock mass-casualty exercise planned at Camp Gruber.** Disease, disaster and terrorists are among the catastrophic events that area emergency response personnel are preparing for during an upcoming training exercise presented at Camp Gruber. The medical-response exercise in June there involves more than 200 people from Oklahoma, Arkansas, Texas and Mississippi. Organized by staff at the Jack C. Montgomery VA Medical Center, the "Medical Patriot Operational Readiness Test" will help area medical people assess their preparation to handle something like another Hurricane Katrina, or worse. The emergency management specialist and event co-coordinator said participants will be pushed beyond their limits. "In operational readiness testing, you stress your participants as much as you can," he said. "We will be taking an all-hazardous approach. That means simulating smallpox, avian flu and something chemical." The test is designed to be more complex than a real event, he said. There may also be participants pretending to be terrorists who will try to attack the medical facilities. He said one goal is to deploy federal medical assets and integrate them with community operations. There will be three days of training before the final exercise on June 20.
Source: http://www.muskogeephoenix.com/local/local_story_098003926.html

[Return to top]

Information Technology

28. *April 8, Techworld* – (International) **Outsourcing blamed for rising security woes.** The world has a new culprit to blame for the rising tide of software vulnerabilities – code outsourcing. The trend to outsource the coding of applications is now a major contributor to making business software more vulnerable, a survey-cum-report by analyst group Quocirca has claimed. According to their survey of 250 IT directors and executives in the US, the UK and Germany for Fortify Software, ninety percent of the organizations that admitted to having been 'hacked' had outsourced more than 40 percent of their applications to third parties. The rush to benefit from the speed, convenience and lower cost of outsourced applications left security as an afterthought in an alarming number of cases. Sixty percent of respondents reported not mandating security from scratch, while 20 percent of those surveyed in the UK failed to accommodate security at all in the outsourced applications. The report mainly blames the way companies have become enamored with relatively poorly-understood Web 2.0 technologies, and the parallel rush to use service-oriented architectures (SOA) to open up software to partners. As to outsourcing itself, according to Fortify, the problem here is that the client company has no visibility on the coding behavior of the company carrying out the work, no matter how good the relationship appears to be. "These survey results help explain the recent, sudden rise in data breaches and should serve as a wake-up call to any executive whose company sits on a pile of mission-critical application code," said a Fortify board member and former White House cyber-security advisor. Source: http://www.techworld.com/news/index.cfm?newsID=11922&printerfriendly=1

29. *April 8, Computerworld* – (International) **Malware count blows past 1M mark.** Symantec Corp.'s malware tally topped 1 million for the first time in the second half of 2007 as the number of new malicious code threats skyrocketed, the company said in its semiannual report on the state of security. Of the 1.1 million code threats that Symantec has detected since it began writing signatures more than a quarter-century ago, 711,912 were discovered in 2007; 499,811 were picked up in the last six months of the year alone. In other words, nearly two-thirds of all the threats that Symantec has ever uncovered were found last year. Symantec credited the explosion in threats to a shift to specialization by malware makers and the existence of well-oiled – and well-financed – organizations that hire those programmers to write exploits and craft attacks. "This [six-month] reporting period has seen the strongest evidence yet of this," said a senior research manager with Symantec's security response team. He ticked off a slew of traits now common in the malware industry, from the development of what he called "crime management kits" to proof that hackers work in a market-driven economy where threats are the coin of the realm. He called 2007's tsunami of threats a "tipping point," and said that it is clear that security vendors –and their users – will soon need to switch to "whitelisting" legitimate code rather than "blacklisting" threats, as is now the practice. Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9075518&source=rss_topic17

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

30. *April 8, IDG News Service* – (International) **Browser hack renders routers insecure.** A security researcher plans to show how a web-based attack could be used to seize control of certain routers. The researcher, also the director of penetration testing at IOActive, has spent the past year studying how design flaws in the way that browsers work with the Internet's Domain Name System (DNS) can be abused in order to get attackers behind the firewall. At the RSA Conference in San Francisco, he will demonstrate how this attack would work on widely used routers, including those made by Cisco's Linksys division and D-Link. The technique, called a DNS rebinding attack, would work on virtually any device, including printers, that uses a default password and a web-based administration interface, he said. The victim would visit a malicious web page that would use JavaScript code to trick the browser into making changes on the web-based router configuration page. The JavaScript could tell the router to let the hacker remotely administer the device, or it could force the router to download new firmware, again putting the router under the hacker's control. Either way, the attacker would be able to control his victim's Internet communications. The technical details of the attack are complex, but essentially the attacker is exploiting the way the browser uses the DNS system to decide what parts of the network it can reach. Although security researchers had known that this type of hack was theoretically possible, the demo will show that it can work in the real world, said the CEO of DNS service provider OpenDNS.
Source: http://www.techworld.com/news/index.cfm?newsID=11911&printerfriendly=1

[Return to top]

Commercial Facilities Sector

Nothing to Report

[Return to top]

National Monuments & Icons Sector

Nothing to Report

[Return to top]

Dams Sector

31. *April 8, Examiner* – (Virginia) **Fairfax County seeks federal funds for dam upgrades to safeguard area.** Fairfax County, Virginia, is asking Congress to restore millions of dollars worth of funding for dam upgrades so it can meet more stringent state standards and protect downstream communities in the Burke area. Fairfax wants to improve dams in Woodglen Lake and Lake Barton next year, as well as at Huntsman Lake the following year. The upgrades are needed to safeguard 3,200 residents and property worth more than $300 million in the downstream communities, wrote the Board of Supervisors chairman. The tougher requirements are an outgrowth of studies in the late 1990s that showed the potential for spillway erosion during a major storm, said the Fairfax County director of storm-water planning.
Source: http://www.examiner.com/a-1326718~Fairfax_County_seeks_federal_funds_for_dam_upgrades_to_safeguard_area.html?cid=rss-Washington_DC

32. *April 7, WPMI 15 Mobile* – (Florida) **Temporary dam breaks following heavy rains.** Rising waters in Locklin Lake in the central part of Milton, Florida, overwhelmed a temporary dam during heavy rains on Saturday morning. The temporary dam was in place during work to repair the permanent dam. Monday, city crews were busy digging out concrete slabs which were part of the new temporary dam under construction. Two homes downstream were damaged by the rushing waters. There was minor flooding in one home and the other had damage to its yard and fence. Workers will replace the damaged wall with another ten-foot-tall temporary dirt dam until work is complete on the permanent dam in November.
Source: http://www.nbc15online.com/news/local/story.aspx?content_id=90b6025a-0cd1-4cdd-9ad7-5c2e8616c5c2&rss=217

[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.