Department of Homeland Security Daily Open Source Infrastructure Report for 06 August 2007

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

Daily Highlights

- The FBI and Homeland Security agents are investigating several incidents of laser beams being shined into cockpits of landing planes at the Daytona Beach Airport in Central Florida. (See item 14)
- Department of Transportation Secretary Mary E. Peters on has called on all states to immediately inspect any steel deck truss bridges similar to the I−35 bridge that collapsed Wednesday night in Minneapolis. (See item 15)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

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. *August 04, Dow Jones* — **House passes renewable electricity standard.** The U.S. House of Representatives passed a bipartisan amendment to a broad energy package Saturday, August 4, requiring utilities to provide 15 percent of their power from renewable energy sources by 2020. Inclusion of a renewable power standard −− approved by a vote of 220−190 −− is a major addition to the kind of energy package the House and Senate Democratic leadership is seeking, especially after a similar bill failed to pass in the Senate. Both the White House and the electricity industry are strongly opposed to the Renewable Electricity Standard, saying that it would raise electricity prices and put unequal burdens on states that weren't naturally

predisposed for such renewable sources as wind and solar energy. The bill will impact investor−owned utilities, such as Exelon Corp., TXU Corp. and Entergy Corp., and not co−ops or municipal utilities. Analysts say it will also positively impact companies such as Renewable Energy Corp., which produces solar chips and cells, and wind turbine manufacturers, such as Vestas Wind Systems A/S. Utilities located in areas of the country with few approved renewable resources will be required to purchase credits from utilities located in areas with strong renewable resource potential.
Source: http://online.wsj.com/article/SB118626157965588432.html?mod= googlenews_wsj

2. *August 03, World Nuclear News* — **'Radioactive Boy Scout' arrested.** David Hahn, 31, from Clinton Township, MI, has been accused of stealing smoke detectors containing americium. Hahn was previously described as "The Radioactive Boy Scout" after trying to make a thorium−based reactor in a shed at his mother's home when a 17−year old. Now 31, Hahn, was being held in the Macomb County Jail on charges of larceny from a building. After Hahn was arrested police searched his home. They found 16 smoke detectors. Police suspect Hahn was trying to extract the tiny amounts of americium−241 used in the smoke detectors. Amercium−241 is a radioactive silvery−white metal. Hahn was first caught dealing with radioactive materials by police in 1994. He was driving a car containing components from a failed attempt to make a homemade nuclear reactor using traces of thorium extracted from camping gas mantles. Although the attempts were futile, Hahn became alarmed by the higher than background radiation levels and dismantled his apparatus and stored them in a toolbox. Subsequently, the shed at his mother's home was designated a hazardous materials cleanup site and was dismantled and disposed of as low−level radioactive waste.
Source: http://www.world−nuclear−news.org/regulationSafety/Former_Radioactive_Boy_Scout_arrested_for_stealing_smoke_detectors−03 0807.shtml

3. *August 01, NBC (WI)* — **Theft of radioactive device prompts concern; reward being offered.** A radioactive device is missing from an oil pipeline construction site in Wisconsin. Police say it's one of a number of items stolen but the most dangerous. The theft happened sometime early Tuesday morning, July 31, and it's significant enough to get the state and the FBI involved in the investigation. "The lock had been cut off of the door, trailer been ransacked. There was lots of things missing," says George Thornton with WeldSonix out of Houston. One of the things missing is called a masterminder. "It's the size of a two−pound coffee can ... handle on the top," Adams County Emergency Management Coordinator Jane Grabarski says. Investigators want to get their hands on it because it's radioactive. "It doesn't look real threatening, but it does have a container that's dangerous to the public," she says. Thornton says he and his crews work on an oil pipeline under construction from Superior to Illinois. The masterminder was in a trailer at a work site near the Town of Rome when thieves took off with it. He says the device's outer container was marked as having radioactive material inside of it.
Source: http://www.nbc15.com/news/headlines/8859237.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

4. *August 02, Government Accountability Office* — **GAO−07−1029R: DoD Is Making Progress in Adopting Best Practices for the Transformational Satellite Communications System and Space Radar but Still Faces Challenges (Correspondence).** The Department of Defense (DoD) is working to achieve information superiority over adversaries and share information seamlessly among disparate weapons systems. Two programs envisioned as a part of this effort are Transformational Satellite Communications System (TSAT) and Space Radar. TSAT is designed to provide rapid worldwide secure communications with air and space systems through radio frequency and laser communications links. Space Radar is expected to provide global all−weather intelligence, surveillance, and reconnaissance, particularly in denied areas, for military, national intelligence, and civil users. Both TSAT and Space Radar will require major software development efforts and employ a significant number of experienced staff. The Government Accountability Office (GAO) was requested to assess DoD's progress in adopting best practice as both of these programs proceed toward product development. GAO presented their findings on TSAT and Space Radar in briefings in March 2007. This letter summarizes GAO's findings, conclusions, and recommendations.
   Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−1029R

5. *July 06, Government Accountability Office* — **GAO−07−929R: Sales of Sensitive Military Property to the Public (Correspondence).** Each year the Department of Defense (DoD) sells millions of dollars worth of excess property to the public through a Website run by its contractor, Government Liquidation. Before excess property can be sold on this site, it is DoD policy to screen the property to ensure it cannot be reutilized by the department in another location or that its sale would not result in sensitive military property becoming publicly available. DoD assigns demilitarization codes to sensitive military property so that it is recognized and disposed of properly. However, on several prior occasions −− most recently at a July 2006 hearing −− the Government Accountability Office (GAO) reported that management control breakdowns in DoD's excess property reutilization program resulted in the sale of sensitive military property to the public through the liquidation Website, including property subject to demilitarization controls such as F−14 aircraft parts. Given the seriousness of the security risk posed by the sale of sensitive military property to the public, the GAO was requested to investigate whether (1) demil−required property was still being sold on DoD's contractor−run liquidation Website and (2) whether DoD has taken steps to prevent further improper sales of sensitive items, including controlled and demil−required property.
   Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−929R

[Return to top]

Banking and Finance Sector

6. *August 03, Associated Press* — **Computer security problems found at IRS.** IRS employees ignored security rules and turned over sensitive computer information to a caller posing as a technical support person, according to a government study. Sixty−one of the 102 people who

got the test calls, including managers and a contractor, complied with a request that the employee provide his or her user name and temporarily change his or her password to one the caller suggested, according to the Treasury Inspector General for Tax Administration (TIGTA), an office that does oversight of Internal Revenue Service. The caller asked for assistance to correct a computer problem. The report said that by failing to question the identity of the caller the employees were putting the IRS at risk of providing unauthorized people access to taxpayer data that could be used for identity theft and other fraudulent schemes. Only eight of the 102 employees contacted either the inspector general's office or IRS security offices to validate the legitimacy of the caller.
TIGTA Report: http://www.treas.gov/tigta/auditreports/2007reports/200720107_oa_highlights.pdf
Source: http://news.yahoo.com/s/ap/20070803/ap_on_hi_te/irs_computer_security;_ylt=ApaeBHQGoRnW5joZkaFQSwcjtBAF

7. *August 03, Finextra* — **Australian banks hit by tech glitches.** Commonwealth Bank of Australia (CBA) and Bank of Queensland (BoQ) were both hit by systems failures last week, according to press reports. CBA's software provider Oracle is reportedly working to fix a glitch that has caused "extensive problems" with the bank's CommSee teller system and online business banking application CommBiz. The glitch, which occurred after a routine upgrade of the Oracle platform, has resulted in delays for retail customers getting loan approvals and opening new accounts at branches. According to press reports Oracle was forced to fly software experts into the country to help fix the problem. CBA has told its business customers to avoid using the CommBiz platform until the problem has been fixed. Meanwhile BoQ has been working to fix technical problems with its Internet banking service that prevented some customers from accessing their accounts. The problem, which follows recent routine upgrades to the system, has left the bank's online services congested and unable to operate at full capacity at peak times.
   Source: http://www.finextra.com/fullstory.asp?id=17276

8. *August 02, ComputerWorld* — **With ID theft, fraud fears growing, credit cards ranked on security.** A new study of credit cards from 25 of the largest issuers found that many still fall short of protecting users from fraud. The report, released by Javelin Strategy & Research, found that while almost all card issuers do well in helping their customers after fraud or theft occurs, many need to upgrade their identity fraud detection tools. Among the key deficiencies: 56 percent of the 25 card issuers surveyed continue to require full Social Security numbers to help identify their customers, whether by phone, online or by mail. Consumers are not allowed to set transaction limits or block certain types of transactions using their credit cards, such as restricting card use to purchases only made with U.S. vendors, according to the study. In fact, only 24 percent of the surveyed card issuers allow consumers to set so−called user−defined limits and/or prohibitions on their accounts to help prevent unauthorized use, the study concluded. While more card issuers now offer consumers e−mail or telephone "transaction alerts" to advise them of account activity, the number of participating card companies is still small −− about 8 percent.
   Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9028780&intsrc=hm_list

[Return to top]

Transportation and Border Security Sector

9. *August 05, Associated Press* — **Train gets stuck in Penn Station tunnel.** A commuter train carrying 900 passengers was evacuated after it got stuck heading into a tunnel at Pennsylvania Station early Sunday, August 5, authorities said. No injuries were reported. Damage to overhead wires brought the electric−powered, Trenton, NJ−bound NJ Transit train to a halt around 12:45 a.m. EDT, spokesperson Dan Stessel said. He said the train stopped about 200 feet from the Penn Station platform, and only some cars were in the Amtrak−operated tunnel. Passengers transferred to another train that pulled up directly behind the disabled one, Stessel said. They were brought back to Penn Station and boarded another train that left for Trenton at 2:50 a.m. on a different track, he said. Crews were working to fix the stranded train, and normal NJ Transit service was expected to continue, Stessel said.
Source: http://hosted.ap.org/dynamic/stories/B/BRF_TRAIN_STUCK?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

10. *August 04, WTVJ (FL)* — **Passenger at MIA says two men talked of hijacking.** Two men were removed from a plane at Miami International Airport (MIA) Friday night, August 3, when a passenger alerted authorities and said she overheard them saying they had planned to hijack the plane. The incident occurred around 10 p.m. EDT on board American Airlines flight 936 from MIA to Hartford, CN. The flight never left the gate. The two men were removed and questioned. K−9 units searched the plane and the flight was given an all−clear to take off.
Source: http://www.nbc6.net/news/13819595/detail.html

11. *August 03, Associated Press* — **Scare in New York harbor.** On the morning after his arrest in New York Harbor, the skipper of a ramshackle replica of a Revolutionary War−era, wooden hulled submarine found himself splashed across the city's front pages Saturday in less than flattering terms. Philip "Duke" Riley, 35, was surrounded by officers of the police harbor unit and the Coast Guard on Friday morning, August 3, after two friends towed his plywood and fiberglass replica of the 1776 "Turtle" submarine toward the luxury ocean liner Queen Mary 2. It may not have been the brightest idea in security conscious, post−9/11 New York. Riley was taken into custody and his floating homage to the spirit of 1776 was impounded. He was hoping to get videotape of his tiny, egg−shaped sub against the towering majesty of the ocean liner for one of his upcoming shows. He got within 200 feet of the ship's bow before a detective with the NYPD Intelligence Division spotted the partially submerged sub violating the security zone around the Queen Mary. The Coast Guard issued citations for an unsafe vessel and violating a security zone, and the city police ticketed him for reckless operation of a craft and towing in a reckless manner. Riley's two friends escaped unscathed.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/08/04/AR2007080400241.html

12. *August 03, Associated Press* — **Sensors might detect bridge crises.** Researchers at Los Alamos National Laboratory in Albuquerque, NM, are hoping small sensors put on bridges −− about the size of a credit card and costing only $1 apiece −− could provide an early warning to potential failures like the one in Minneapolis. Los Alamos scientists, in collaboration with the University of California at San Diego, say such a system would provide enough lead time to either shut down a bridge or perform preventive maintenance to avert serious failures. "The

idea is to put arrays of sensors on structures, such as bridges, and look for the changes of patterns of signals coming out of those sensors that would give an indication of damage forming and if it is propagating," said Chuck Farrar, a civil engineer at the lab. The electronic sensors would be powered by microwaves or the sun and would send data via radiotelemetry to a computer for analysis. The sensors detect electrical charges emitted by stress on material, such as steel−reinforced concrete. Researchers are in the second year of the four−year project −− funded at $400,000 a year −− and it probably will be years before the sensors are commercially available, Farrar said.
Source: http://hosted.ap.org/dynamic/stories/B/BRIDGE_COLLAPSE_SENSORS?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

13. *August 03, Associated Press* — **FAA: US Airways pilot took wrong turn at Philadelphia airport.** A US Airways pilot is under investigation for veering his jet into the path of another airplane over the weekend, federal authorities said Thursday, August 2. A US Airways flight from Las Vegas landed shortly before midnight Sunday, July 29, at the Philadelphia International Airport. The pilot was told by air traffic controllers to take a right on a taxiway, said Arlene Salac, a spokesperson for the Federal Aviation Administration (FAA). Instead, the pilot took a left and crossed over a runway being used by an Air Wisconsin flight to Cincinnati. Air traffic controllers told the Air Wisconsin pilot to turn at the closest taxiway to avoid a collision. A preliminary report shows that over 1,000 feet separated the two planes, Salac said.
Source: http://www.usatoday.com/travel/flights/2007−08−03−usairways− miss_N.htm

14. *August 03, Local6 (FL)* — **Laser beams aimed into cockpits near Florida airport.** The FBI and Homeland Security agents are investigating several incidents of laser beams being shined into cockpits of landing planes in Central Florida. Investigators said pilots have reported a thin beam of light being targeted into the cockpits of their planes near the Daytona Beach Airport. One of the planes was attempting to land at the airport when it was targeted. "These are sensitive times and pointing anything at a flying aircraft, even from a distraction standpoint is still a safety risk," Embry Riddle Aeronautical School representative Frank Ayers said. During one of the incidents, the pilot maneuvered away from the light on final approach to the airport. The incidents have happened two nights in a row, authorities said.
Source: http://www.local6.com/news/13817679/detail.html

15. *August 02, Department of Transportation* — **Secretary of Transportation calls on states to immediately inspect all steel arch truss bridges.** Department of Transportation Secretary Mary E. Peters on Thursday, August 2, called on all states to immediately inspect any steel deck truss bridges similar to the I−35 bridge that collapsed Wednesday night in Minneapolis. "Even though we don’t know what caused this collapse, we want states to immediately and thoroughly examine all similar spans out of an abundance of caution,” said Peters. According to Federal Highway Administration (FHWA) data, there are 756 of the relatively unique steel deck truss bridges in the United States. The Federal Highway Administration issued the guidance to all state transportation agencies and bridge owners strongly advising them to conduct an inspection or, at minimum, review inspection reports to determine if further action is needed.
FHWA list of steel deck truss bridges: http://www.fhwa.dot.gov/
Source: http://www.dot.gov/affairs/fhwa1207.htm

16. *August 02, Department of Transportation* — **Secretary Peters asks Inspector General to review the National Bridge Inspection Program.** In response to the tragic bridge collapse in Minneapolis Wednesday night, August 1, Department of Transportation Secretary Mary E. Peters has requested the Department of Transportation's Inspector General to conduct a rigorous assessment of the National Bridge Inspection Program. "What happened in Minnesota is simply unacceptable. We must have a top−to−bottom review of the bridge inspection program to make sure that everything is being done to keep this kind of tragedy from occurring again," Secretary Peters said. The Secretary called for the Inspector General to determine if the current federal program delivers the highest level of bridge safety. And, if needed, the Inspector General will make recommendations for future changes to the program.
Source: http://www.dot.gov/affairs/dot7507.htm

17. *July 13, Government Accountability Office* — **GAO−07−870: Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US−VISIT Program (Report).** Intended to enhance the security of U.S. citizens and visitors, United States Visitor and Immigrant Status Indicator Technology (US−VISIT) program encompasses the pre−entry, entry, status management, and exit of foreign national travelers who enter and leave the United States at 285 air, sea, and land ports of entry. The Government Accountability Office (GAO) was asked to determine whether Department of Homeland Security (DHS) has implemented appropriate controls to protect the confidentiality, integrity, and availability of the information and systems used to support the US−VISIT program. To do this, GAO examined the controls over the systems operated by Customs and Border Protection (CBP) that support the US−VISIT program. GAO recommends that the Secretary of Homeland Security direct CBP to fully implement information security program activities for systems supporting the US−VISIT program. In commenting on a draft of this report, DHS stated that it has directed CBP to complete remediation activities to address each of the recommendations.
Highlights: http://www.gao.gov/highlights/d07870high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−870

18. *July 13, Government Accountability Office* — **GAO−07−847: Border Security: Long−Term Strategy Needed to Keep Pace with Increasing Demand for Visas (Report).** After the 9/11 terrorist attacks, Congress and the Department of State (State) initiated changes to the visa process to increase security, but these changes also increased the amount of time needed to adjudicate a visa. Although maintaining security is of paramount importance, State has acknowledged that long waits for visas may discourage legitimate travel to the United States, potentially costing the country billions of dollars in economic benefits over time, and adversely influencing foreign citizens' opinions of our nation. The Government Accountability Office (GAO) testified in 2006 that a number of consular posts had long visa interview wait times. This report examines (1) State's data on visa interview wait times, (2) actions State has taken to address wait times, and (3) State's strategy for dealing with projected growth in visa demand. To improve State's oversight and management of visa−adjudicating posts −− with the goal of facilitating legitimate travel while maintaining a high level of security to protect our borders −− GAO is recommending that State (1) develop a strategy to address worldwide increases in visa demand, (2) improve the reliability and utility of visa waits data, and (3) identify and disseminate practices and procedures used by posts to manage workload and reduce wait times. State concurred with our recommendations.

Highlights: http://www.gao.gov/highlights/d07847high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−847

[Return to top]

Postal and Shipping Sector

19. *August 03, KETV (NE)* — **Nebraska post office reopens after scare.** The Postal Service building at Girls and Boys Town near Omaha was evacuated and shut down for about 90 minutes on Friday morning, August 3, as investigators responded to the report of a suspicious substance. At about 10:30 a.m. CDT, a postal carrier told colleagues that he came in contact with a powder found at the bottom of a carrying crate. The powder was described as a Gatorade−like substance and the worker said his nose burned when he found it. "There was no package attached to it −− nothing associated with it," said Postmaster EvaJon Sperling. "It was not an envelope." The worker was driven to a local hospital, treated and released. Routes that run out of the facility were delayed by a couple of hours as investigators worked. A hazardous materials crew was called. The all−clear was given and the post office reopened shortly after noon.
Source: http://www.ketv.com/news/13814148/detail.html

[Return to top]

Agriculture Sector

20. *August 03, Associated Press* — **Foot−and−mouth disease detected in cattle in southern England.** Cattle on a farm in southern England have been found to be infected with foot−and−mouth disease (FMD), British authorities said Friday, August 3. The Department of Environment, Food and Rural Affairs, or DEFRA, said animals on a farm near Guildford, in Surrey, had tested positive for the highly infectious disease, which affects cows, horses, sheep and pigs. Authorities imposed a two mile radius protection zone and a surveillance zone of six miles around the farm. DEFRA said a ban was also imposed nationwide on moving all hooved animals, including pigs. An outbreak of foot−and−mouth disease last developed in Britain in 2001, leading to the slaughter of seven million animals.
Source: http://www.iht.com/articles/ap/2007/08/03/europe/EU−GEN−Britain−Foot−and−Mouth.php

21. *August 02, Northern Illinois University* — **New ag−weather Website predicts pest migrations.** Farmers have long known the breeze can carry crop−damaging bugs. Now a new Website launched by Northern Illinois University tells agricultural producers in the Midwest which way the wind blows and when pests might be hitching a ride. The agriculture weather site produces a daily Insect Migration Risk Forecast, geared for farmers, agricultural producers and entomologists.
Source: http://www.niu.edu/PubAffairs/RELEASES/2007/aug/bugforcast.s html

22. *August 02, Iowa State University* — **Research sheds light on molecular changes during Asian soybean rust infection.** An extensive analysis of molecular changes that occur while a

plant is being infected by the Asian soybean rust fungus reveals new information that could lead to a soybean variety with broad−spectrum resistance. Iowa State plant pathologists Thomas Baum, Steve Whitham and Martijn van de Mortel led the three−year research project, which is the largest molecular study of the interaction of soybean and Asian soybean rust. The researchers sprayed Asian soybean rust spores on two soybean varieties − a highly susceptible variety and a resistant one in which the disease progresses slowly. Samples were taken every six hours for the first 24 hours and at greater increments of time throughout the next seven days. Then the researchers took genetic material that provided a snap shot of the level of gene expression at the time the plants were sampled. They profiled the gene expression of more than 30,000 soybean genes in each sample. The analyses showed that both varieties immediately responded to the fungus as indicated by significant changes in gene expression levels. Then something unexpected happened. "Twenty−four hours into the infection, gene expression returned to the baseline −− the plant's response to the rust pathogen essentially turned off," Whitham said.
Source: http://www.iastate.edu/~nscentral/news/2007/aug/asianrust.sh tml

[Return to top]

Food Sector

23. *August 03, Reuters* — **House bill directs FDA to revamp food safety work.** The U.S. House passed a $90.7 billion funding bill on Thursday, August 2, that orders the U.S. Food and Drug Administration (FDA) to write a plan for improving its food safety work, brought into doubt by tainted imports this year. Under the bill, which was sent to the Senate, the FDA would submit the plan to Congress early next year with implementation due by July 2009. The House bill calls on the FDA to set clear goals for a multi−year overhaul of its food safety operations. Key components could include enforceable standards for food safety, use of systems like the Hazard Analysis Critical Control Point, and review of safeguards in food−exporting countries.
Source: http://www.reuters.com/article/healthNews/idUSN0222710920070 803

24. *August 02, Associated Press* — **Shellfish poisoning hospitalizes four.** Four people were hospitalized with paralytic shellfish poisoning after eating contaminated mussels, officials said Wednesday, August 1. The incident marked the first case since at least 1980 in Maine. Lobsterman Randy Beal and wife Brenda from Harrington were in critical condition Wednesday evening at Eastern Maine Medical Center in Bangor, a nursing supervisor said. The source of the mussels was not a mussel bed but rather a 55−gallon plastic barrel that was found floating off the coast by Randy Beal. He scraped mussels off the side of the barrel and took them home for a meal. After the family took ill, samples of the mussels were taken from the home, tested and found to be contaminated with a marine biotoxin, commonly called "red tide," associated with algae blooms in ocean waters that can cause paralytic shellfish poisoning. The Beals and a third family member who was in fair condition were hospitalized at Eastern Maine Medical after the incident. The fourth victim was at Down East Medical Center in Machias, but the condition was unavailable.
Source: http://pressherald.mainetoday.com/story.php?id=124666&ac=PHn ws

25. *August 02, Bloomberg News* — **Drug−tainted Asian fish slip into U.S., states find.** Joseph Basile, an Alabama state scientist, drops a frozen catfish filet into an industrial food processor

and pulverizes it into a fluffy white powder. The grinding in a laboratory in Montgomery is part of a test of imported seafood for drugs that U.S. regulators say can cause cancer or increase resistance to antibiotics. Alabama officials have reported finding banned medicines missed by the U.S. Food and Drug Administration (FDA) in seafood from China, Vietnam and other Asian countries. Mississippi, Arkansas and Louisiana also have found banned drugs in imported seafood, according to statements by regulators in those states. Of 94 samples of Chinese catfish checked by Alabama since March, the state reports that 41 tested positive for fluoroquinolones, antibiotics banned in the U.S. for seafood. Of 13 more samples of species similar to catfish, including one called basa, five tested positive for the antibiotic. The exporting countries included Vietnam, Thailand and Malaysia.
Source: http://www.bloomberg.com/apps/news?pid=20601109&sid=aRTNXIGwPyOc&refer=home

26. *August 01, U.S. Food and Drug Administration* — **Green beans recalled.** Lakeside Foods, Inc. of Manitowoc, WI, is initiating a voluntary recall of 15,000 cases of 14.5−ounce French Style Green Beans because some cans may have been under processed and some cans may have leaked. While no illnesses have been reported these cans have the potential to be contaminated with harmful organisms including Clostridium botulinum. No botulinum toxin has been found in any cans tested to date, however the company continues to test out of an abundance of caution. Botulism, a potentially fatal form of food poisoning, can cause the following symptoms: general weakness, dizziness, double vision and trouble with speaking or swallowing. Difficulty in breathing, weakness of other muscles, abdominal distention and constipation may also be common symptoms. The product was distributed in the following 20 states AL, AZ CO, FL, GA, IL, IN, KS, KY, MI, MO, MS, NC, NY, OH, OK, TN, TX, VA, WI and Canada.
Source: http://www.fda.gov/oc/po/firmrecalls/lakeside08_07.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

27. *August 03, Agence France−Presse* — **India's battle against polio making headway.** India's fight against the most dangerous strain of polio appears to be making headway with a sharp fall in the number of cases reported so far this year, according to a report Friday, August 3. Only 39 cases of the fast−moving and virulent P1 strain were recorded in the past seven months from eight states in the country, a health official told the Press Trust of India news agency. That compared with 648 P1 cases reported for 2006, the news agency said. Overall there have been 124 cases of polio reported from eight states, PTI said. Last year, India had a total of 676 cases, up from a low of 66 registered with the health ministry in 2005.
Source: http://news.yahoo.com/s/afp/20070803/hl_afp/healthindiapolio_070803103229

28. *August 03, World Health Organization* — **Marburg hemorrhagic fever in Uganda.** Marburg hemorrhagic fever (MHF) has been confirmed in a 29−year−old man in Uganda. The man became symptomatic on July 4, was admitted to hospital on July 7 and died on July 14. The disease was confirmed by laboratory diagnosis on July 30. The man had had prolonged close contact with a 21−year−old co−worker with a similar illness to whom he had been providing care. The 21−year−old had developed symptoms on June 27 and was hospitalized with a hemorrhagic illness. He then recovered and was discharged on July 9. Both men were working in a mine in western Uganda. Interviews conducted with the mine authorities have identified one additional suspected case and two individuals who were taken ill in mid−June and have since recovered. These individuals are being investigated as a matter of priority. All the miners under investigation for MHF had been at the mine for approximately eight months with no movements outside the mining area during that time. To date, there have been no reported cases among health care workers.
Marburg hemorrhagic fever information:
http://www.who.int/csr/disease/marburg/en/index.html
Source: http://www.who.int/csr/don/2007_08_03/en/index.html

29. *August 02, BMC Infectious Diseases* — **U.S. medical resident familiarity with national tuberculosis guidelines.** The ability of medical residents training at U.S. urban medical centers to diagnose and manage tuberculosis cases has important public health implications. Researchers assessed medical resident knowledge about tuberculosis diagnosis and early management based on American Thoracic Society guidelines. A 20−question tuberculosis knowledge survey was administered to 131 medical residents during a single routinely scheduled teaching conference at four different urban medical centers in Baltimore and Philadelphia. Survey questions were divided into five different subject categories. The median percent of survey questions answered correctly for all participating residents was 55 percent. Medical resident knowledge about tuberculosis did not improve with increasing post−graduate year of training or greater number of patients managed for tuberculosis within the previous year. Common areas of knowledge deficiency included the diagnosis and management of latent tuberculosis infection (median percent correct, 40.7 percent), as well as the interpretation of negative acid−fast sputum smear samples.
Source: http://www.biomedcentral.com/content/pdf/1471−2334−7−89.pdf

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

30. *August 04, Boston Globe* — **Digital age spawns a new first−responder.** When a bridge over the Mississippi River collapsed in Minneapolis on Wednesday, August 1, bystanders raced to the scene to offer assistance, and to document the tragedy for the world. Citizens with digital cameras had posted hundreds of images of the wreckage to Internet photo−sharing sites within

hours of the tragedy. Such photos aren't just personal documents; at a news conference, investigators at the National Transportation Safety Board asked to hear from people who had their cameras trained on the bridge at the moment it fell. Several people have responded so far, and the agency hopes their photos will yield clues to the collapse. It's the most recent example of a transformation in the way we think about disasters. The term "first−responder" officially means the police, fire, and rescue workers who come to the aid of victims. But the digital age has given rise to a new kind of first−responder −− ordinary citizens with cell phones, computers, and Internet access. These people leap into action without being asked. They shoot snapshots and video of ongoing disasters. And they set up instant social networks that provide vital information to the public, the news media, and even the government.
Source: http://www.boston.com/news/nation/articles/2007/08/04/digital_age_spawns_a_new_first_responder/

31. *August 04, PC World* — **Wi−Fi helps in bridge rescues.** A new Wi−Fi network in Minneapolis −− only partially completed and just two months old −− is nonetheless giving the city critical help in responding to the collapse of the I−35W bridge. The network helped the city with communications, moving large mapping files to the recovery site, and is supporting wireless cameras that are being installed to help with recovery operations. "Thank goodness we had it in and that this piece of the network was already up and operational," said Minneapolis City CIO Lynn Willenbring. "We could not have been as effective if it were not for that." The city's IT department immediately went to work to provide basic support and desk−side services for the city's emergency operations command center. The city's geographic information system staff also worked through the night to prepare maps, both for public use and internally to assist with traffic and recovery efforts, she said.
Source: http://www.pcworld.com/article/id,135531−c,currentevents/article.html

32. *August 03, Federal Emergency Management Agency* — **President declares major disaster for Vermont.** The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Friday, August 3, that federal disaster aid has been made available for the state of Vermont to supplement state and local recovery efforts in the area struck by severe storms and flooding during the period of July 9−11, 2007. FEMA Administrator David Paulison said the assistance was authorized under a major disaster declaration issued for the state by President Bush. The President's action makes federal funding available to state and eligible local governments and certain private nonprofit organizations on a cost−sharing basis for emergency work and the repair or replacement of facilities damaged by the severe storms and flooding in the counties of Orange, Washington, and Windsor.
Source: http://www.fema.gov/news/newsrelease.fema?id=38414

[Return to top]

Information Technology and Telecommunications Sector

33. *August 03, eWeek* — **IBM to acquire data management specialist.** IBM is buying Princeton Softech, a privately held company specializing in data archiving, test data management, data privacy, and data classification and discovery software. The financial details of the deal, which was announced Friday, August 3, were not disclosed. Officials at IBM said the acquisition of the company is a key part of IBM's Information on Demand business initiative, meant to help

customers by addressing the challenge of managing data and improving database performance.
Source: http://www.eweek.com/article2/0,1895,2166092,00.asp

34. *August 02, eWeek* — **Service outages still plague BlackBerry, AT&T.** For companies that pride themselves on service and reliability, AT&T and Research In Motion certainly have had their share of service interruptions, and there seems to be no end in sight. Yet another data outage Wednesday, August 1, although brief, is reported to have affected numerous BlackBerry users nationwide. According to Brad Mays, a spokesperson for AT&T, some of AT&T's EDGE wireless data customers around the country experienced difficulty with the wireless data network for a brief period of time. Voice calling was unaffected, and the company quickly identified the cause of the problem and fixed it.
Source: http://www.eweek.com/article2/0,1895,2165691,00.asp

35. *August 02, InformationWeek* — **DoS attack feared as Storm worm siege escalates.** As the Storm worm grows into a prolonged online siege 10 times larger than any other e−mail attack in the last two years −− amassing a botnet of nearly 2 million computers −− researchers worry about the damage hackers could wreak if they unleash a denial−of−service attack with it. Between July 16 and August 1, researchers at software security firm Postini have recorded 415 million spam e−mails luring users to malicious Websites, according to Adam Swidler, a senior manager with Postini. Researchers at SecureWorks are seeing similar staggering numbers, as well. Joe Stewart, a senior security researcher at SecureWorks, noted that the number of zombie computers that the Storm worm authors have amassed as skyrocketed in the past month. From the first of January to the end of May, the security company noted that there were 2,815 bots launching the attacks. By the end of July, that number had leapt of 1.7 million. And both Stewart and Swidler said they think the Storm worm authors are cultivating such an enormous botnet to do more than send out increasing amounts of spam. All of the bots are set up to launch denial−of−service (DoS) attacks and that's exactly what they're anticipating.
Source: http://www.informationweek.com/management/showArticle.jhtml;jsessionid=ZSI3I0MWJVWLUQSNDLRCKHSCJUNN2JVN?articleID=201202 711

36. *August 01, eWeek* — **Hostway server migration leaves clients in the dark.** A torrent of Website postings to social networking site Digg, along with several quickly erected blogs, reflect a data center migration gone badly awry, leaving thousands of Hostway customer Websites in the dark. Hostway Web hosting customers have posted reports that their Websites and back−office applications have been offline for as long as three days. In April, Hostway joined with Affinity Internet to become one of the largest Web hosting providers in the world, according to the company's Website, with 15 operation centers in 11 countries. Combined, the companies have 600,000 Web hosting customers. The planned July 27 data center migration at ValueWeb, a Hostway company, involved moving more than 3,700 servers 270 miles, from Affinity's Miami hosting facility to a Hostway data center in Tampa, FL, according to Rich Miller, reporter for Data Center Knowledge, in Lawrenceville, NJ. The company notified customers in e−mails that the outage would last between 12 and 15 hours, with an estimated completion time of 7 p.m. EDT on July 28. By July 30, customers posting to a discussion forum on Digg, titled How Not to Migrate a Data Center, said their sites were still down.
Source: http://www.eweek.com/article2/0,1895,2165290,00.asp

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

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS 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 dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 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