Department of Homeland Security Daily Open Source Infrastructure Report for 09 February 2007

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

Daily Highlights

- USA TODAY reports the U.S. government is asking foreign countries to allow pilots to carry guns in the cockpit when they fly overseas, trying to expand a four−year−old program that allows thousands of pilots to carry guns on domestic flights. (See item 17)
- The Transportation Security Administration said Wednesday, February 7, that the nation's 43,000 airport security screeners will now receive notices and photos of abducted children as part of the AMBER Alert network's quest to find missing people. (See item 22)
- The Department of Homeland Security has announced the establishment of the National Advisory Council, which is being created to advise the Administrator of the Federal Emergency Management Agency on all aspects of emergency management in an effort to ensure close coordination with all involved. (See item 36)

DHS Daily Open Source Infrastructure Report *Fast Jump*

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. *February 08, New York Times* — **Lapse in safety procedures adds to debate on New Jersey power plant.** After inspectors found 10 years ago that rust had eaten nearly a third of the way through parts of the steel containment liner that surrounds the Oyster Creek nuclear reactor, the

plant's owner signed an agreement with federal regulators promising to stop further damage. Now, the plant's license is up for renewal before the federal Nuclear Regulatory Commission (NRC), and state records say the owners failed to take all the promised steps to prevent water from reaching the liner. The condition of the liner has been at the center of a dispute over the plant's license application. New Jersey officials have asked the NRC to study the risk the plant poses as a terror threat. While many plants store waste underground, Oyster Creek keeps hundreds of tons of spent nuclear fuel in a pool near the top of its reactor building, which critics say makes it more vulnerable to attack. Company officials said in a recent interview that the pool was still safe, and noted that the plant had extensive security and had passed federal terrorism drills since September 11. The Oyster Creek plant provides about seven percent of the electricity used in New Jersey.
Source: http://www.nytimes.com/2007/02/08/nyregion/08oyster.html?pag ewanted=all

2. *February 08, Windsor Star (Canada)* — **Hacker hits Canada's Nuclear Safety Commission Website.** A brazen hacker attacked the Canadian Nuclear Safety Commission Website Wednesday, February 7, littering it with photographs of a nuclear explosion and raising concerns about the security of information held by the nation's nuclear watchdog. The incident was discovered about 3:00 p.m. local time by an Ottawa Citizen reporter. All of the commission's current and archived news releases, dating back to 1998, were renamed as "security breaches" and when opened, a color photograph of a fiery mushroom cloud appeared under the heading "For Immediate Release." An accompanying caption read: "Please dont (sic) put me in jail ...oops, I divided by zero." The pages were disabled minutes after the newspaper contacted the agency. Commission spokesperson Aurele Gervais said the attack was limited to the Website's public media section and "there's been no internal information that's been compromised."
Source: http://www.canada.com/windsorstar/news/story.html?id=22881f69−eaf2−445a−bc6f−fb7a6753950d

3. *February 07, Vancouver Sun (Canada)* — **BC Hydro lost millions from theft, damage last year.** Thieves raiding BC Hydro installations last year −− three of whom died while one was badly injured −− cost the crown corporation millions of dollars in stolen property and damage, a Hydro official said today. Now Hydro is fighting back and implementing a wide range of deterrent measures to deter thefts of copper wire and equipment including spraying the items favored by thieves with microdots so items can be traced, said Elisha Moreno. "There are microscopic dots that contain a logo or an ID number and these dots can be sprayed on to equipment. They can be viewed through a microscope which will enable us to identify any material that has been stolen from us if it is recovered," she said. Hydro installations in the Lower Mainland and on Vancouver Island are being hit the hardest and anti−theft measures will be directed to these trouble spots first. Better fencing and video surveillance cameras are being mounted in the substations and the locks are being changed on junction boxes after investigators looking into a fatality in Langley found thieves had come up with a way to break the locks.
Source: http://www.canada.com/vancouversun/news/story.html?id=bcd99a54−c509−4d76−9ebf−642b35306df4&k=14848

4. *February 07, Washington Post* — **U.S. seeks partnership with Brazil on ethanol.** The United States and Brazil, the two largest biofuel producers in the world, are meeting this week to

discuss a new energy partnership that they hope will encourage ethanol use throughout Latin America and that U.S. officials hope will diminish the regional influence of oil−rich Venezuela. U.S. officials said they expect to sign accords within a year that would promote technology−sharing with Brazil and encourage more Latin American neighbors to become biofuel producers and consumers. Brazil, the world's largest exporter of ethanol, has been a leader in biofuel technology after its government invested heavily in the ethanol industry in the 1970s. Its sugar cane−based ethanol is more efficient to produce than the corn−based fuel made in the United States. Although the United States has surpassed Brazil in the total amount of ethanol produced, its producers cannot keep up with surging demand. Last year, the United States produced about 4.9 billion gallons and imported an additional 1.7 billion gallons, mostly from Brazil.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/02/07/AR2007020702316.html

5. *February 06, Associated Press* — **At least four injured in California oil field explosion and fire.** Explosions at an oil field Tuesday afternoon, February 6, injured at least four workers, emergency responders and company representatives said. An explosion occurred just before 2:35 p.m. PST at an oil field in Taft, CA about 35 miles southwest of Bakersfield. Several small portable office structures were destroyed, but no major buildings burned, Chris Cagle, an engineer at the Kern County Fire Department. The fire began on a gas line that ruptured and ignited, Cagle said. The exact cause is being investigated. The field is operated by Occidental of Elk Hills, a division of Occidental Petroleum Corporation. The cause of the explosions and the extent of the damage are unknown, but the blasts appear to have originated at and spread from a transportation pipeline. Wells and gas valves in the area were being shut down as a precaution, said Susie Geiger, spokesperson for Occidental of Elk Hills.
Source: http://www.signonsandiego.com/news/state/20070206−1841−oilfi eldfire.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *February 08, Associated Press* — **Plant explosions prompt mandatory evacuations.** Firefighters worked Thursday, February 8, to douse the last of the flames at a chemical distribution business in Kansas City, MO, where several explosions shot fireballs hundreds of feet in the air and sent a vast plume of black smoke drifting over the downtown skyline. Two workers at Chemcentral Corp. suffered minor injuries after several 55−gallon drums of chemicals exploded behind the warehouse Wednesday afternoon, touching off more explosions and fires on the site in a mixed industrial and residential neighborhood northeast of downtown. Police drove through the streets enforcing a mandatory evacuation of homes and businesses within a one−mile radius of the company, which stores and distributes various chemicals and solvents. Despite the smoke plume's ominous appearance, officials reported late Wednesday that tests by the Environmental Protection Agency found no threat to human health. Still, residents were cautioned against picking up any of the debris scattered by the blasts or what appeared to be a sticky substance deposited by the cloud as it streamed southwestward. Eight elementary schools near the business were evacuated after the initial blast, with children still on hand for after−school programs bused to a high school.
Source: http://bob.wjla.com/headlines/0207/395492.html

7. *February 07, KERO−TV 23 (CA)* — **Elk Hills Petroleum blast injures four, destroys two mobile homes.** A huge explosion at the Elk Hills Petroleum Reserve near Taft, CA, on Tuesday afternoon, February 6, sent flames hundreds of feet in to the air and four people to the hospital. At about 2:30 p.m. PST, a natural gas line ruptured, sending flames into the air. The explosion destroyed two mobile homes and forced one man to be airlifted to Kern Medical Center with second−degree and third−degree burns. Three other workers suffered minor injuries. A second explosion occurred at about 5:30 p.m. PST. No one was injured in that blast.
Source: http://www.turnto23.com/news/10946580/detail.html

[Return to top]

Defense Industrial Base Sector

8. *February 08, Aviation Week* — **Analysts see good and bad in defense budget.** The Department of Defense's (DoD) budget is now forecast to grow at a 2.8 percent compound annual growth rate through fiscal 2012, slightly slower than some Wall Street analysts' prior forecast, although still coming off a significantly higher FY '08 baseline budget. In turn, the Bush Administration's Monday, February 5, budget proposal has reconfirmed many analysts' expectation that current and immediate future defense spending will continue at a robust pace, especially for ground forces and even shipbuilding programs, although annual DoD appropriations starting at the end of this decade could draw back. Total proposed FY '08 defense funding −− baseline and supplemental requests −− would be $623 billion, or $27.4 billion, 4.5 percent, greater than the expected $596 billion total this fiscal year, notes Jim McAleese of McAleese & Associates in an analysis with Credit Suisse. The requested growth in FY '08 defense funds would prevent either the Navy or the Air Force from becoming "bill−payers" to support necessary growth in the Army and Marine Corps. David Strauss of UBS Investment Research said related corporate valuations remain sustainable near−term, but they are less certain beyond then and projections could start getting hazy this fall.
Source: http://www.aviationweek.com/aw/generic/story.jsp?id=news/ANA 02087.xml

9. *February 08, CongressDaily* — **Army trims and stretches future combat program.** The Army acknowledged Wednesday, February 7, it sliced $3.4 billion over the next six years from its principal modernization program to fund more immediate needs of the heavily deployed service. The decision to cut Future Combat Systems (FCS) was "strictly budget driven," given the enormity of the Army's needs, service officials said while briefing reporters at the Pentagon. They emphasized that the $160 billion technology transformation program, in development since 2003, is meeting cost goals and is largely on schedule. But faced with budget challenges, the Army last month privately spelled out plans to cut four of the 18 systems intended for FCS. They also chose to stretch out plans for producing and fielding systems by an additional five years, extending production to 2030. "Clearly, we've had to go through a very difficult period here" balancing the current combat forces' needs against the Army's future goals, said Maj. Gen. Jeffrey Sorenson, the Army's deputy for acquisition and systems management. But Sorenson and other senior Army officials insisted that, despite the cuts, the Army will meet all of its basic operational requirements for the program.
Source: http://www.govexec.com/story_page.cfm?articleid=36084&dcn=to daysnews

[Return to top]

Banking and Finance Sector

10. *February 08, Register (UK)* — **Yorkshire Website to aid SMEs in phish fight.** A new Website has been developed to help small and medium enterprises (SMEs) in Yorkshire, UK, protect themselves from cyber crime. Named Yorkshire−Safe, the regional pilot has been developed to provide guidance and an online tool for businesses to check the security of their systems. It also features learning modules to support SMEs in developing their own secure systems. The pilot was announced on Wednesday, February 7, and the Website will eventually be rolled out across England and Europe. Partners include the four Yorkshire police forces, the Serious Organized Crime Agency, Sheffield Hallam University, the Department of Trade and Industry, Mid−Yorkshire Chamber of Commerce and Industry, Yorkshire Forward, and People United Against Crime. The site is multilingual and can be translated into Urdu, Bengali and Polish at the touch of a button. It will soon be available in German, Spanish, French and Italian ready for its European launch.
    Yorkshire−Safe Website: http://www.yorkshire−safe.org/
    Source: http://www.theregister.co.uk/2007/02/08/yorkshire−safe_fight s_cybercrime/

11. *February 08, Associated Press* — **Drug trade said to transform money wires.** Drug money has largely transformed New York's wire transfer industry into a tool of the narcotics trade, federal prosecutors said as they charged 27 wire transfer store owners and employees with money laundering. The 27 people were arrested early Wednesday, February 7, in a series of raids on stores in Queens, Long Island and in Westchester County in which law enforcement agents said they seized about $300,000 in cash, some of which was hidden in ceilings and wall safes. The defendants were accused of laundering a total of $2 million in drug money to Colombia. The raids were part of Operation Pinpoint, the latest phase in an effort to drive drug money out of the wire transfer industry, U.S. Attorney Roslynn Mauskopf said Wednesday.
    Source: http://www.chron.com/disp/story.mpl/ap/fn/4536628.html

12. *February 08, PC Advisor (UK)* — **Banks could pass on phishing losses to customers.** The failure of customers to secure their own money during Internet transactions could potentially lead banks to pass off the responsibility of financial losses back to the customer. User education for online banking customers on how to avoid phishing scams has failed, according to Paul Henry, senior vice president of Secure Computing. Henry said lots of financial organizations have done a great deal of customer education in response to phishing attacks. But it has done very little, Henry said, because commonsense isn't applicable when dealing with phishers. "Even if you manually enter a URL, security is obsolete as phishers have created Trojan code that modifies the host file on Windows to automatically redirect," he said. "Phishers can also attack a router and redirect information to a different server −− user commonsense is no longer valid." Henry said banks are reluctant to refund losses if an account is hijacked. For example, he said a Bank of America customer had a PC compromised with a Trojan losing $90,000 from the account. Although the theft is currently before U.S. courts, Henry said the Bank of America has adopted the attitude that a Trojan on your PC is "your problem."
    Source: http://www.pcadvisor.co.uk/news/index.cfm?newsid=8338

13. *February 07, CNET News* — **UK data thieves face two years in prison.** Individuals who sell or deliberately misuse others' personal data in the UK could now face a penalty of up to two years in prison. The previous penalty stipulated for the charge in the Data Protection Act 1998 was a fine. Now data thieves risk up to six months in prison for a summary conviction, while for a conviction on indictment, they could get up to two years, the UK Department for Constitutional Affairs said Wednesday, February 7. The change comes as the British government moves to increase data sharing as a way of offering higher−quality public services to citizens. The government plans to introduce the amendment to parliament when time allows. Simon Briskman, partner at London law firm Field Fisher Waterhouse, said the new law is positive for businesses worried about data misuse by insiders. "I can only see that better and stronger enforcement plans will help," fight data theft, he said. He stressed the international nature of the problem, citing a recent British TV program, Channel 4's "Dispatches," that said criminal gangs are selling UK credit card and passport details from Indian call centers. Along with tougher penalties, Briskman believes more data theft cases will now come to court.
Source: http://news.com.com/U.K.+data+thieves+face+two+years+in+prison/2100−1029_3−6157219.html

14. *February 07, CNET News* — **Antivirus expert: 'Ransomware' on the rise.** Online criminals are turning away from threatening companies with massive cyberattacks in favor of encrypting a victim's data and then demanding money to decrypt it, an antivirus expert has claimed. Eugene Kaspersky, head of antivirus research at Russia's Kaspersky Labs, told the RSA Conference Tuesday, February 6, that the use of so−called "ransomware Trojans" is a key trend for 2007. This malicious software infects a PC, encrypts some data and then displays an alert telling the victim to send money to get the decryption key needed to access their data again. Such malicious software isn't new. Early examples include Cryzip, discovered in March 2006, and GPCode, discovered in May 2005. Cryzip and GPCode didn't cause massive damage, but Kaspersky believes cybercriminals will refine their use of ransomware Trojans this year. The final version of GPCode used a 660−bit encryption key, which should have taken a single powerful PC around 30 years to crack but was actually broken quickly by Kaspersky Labs, he said.
Source: http://news.com.com/Antivirus+expert+Ransomware+on+the+rise/2100−7355_3−6157092.html

15. *February 07, IDG News Service* — **FTC: Identity theft remains top consumer complaint.** Identity theft remained top of mind among U.S. consumers last year, but complaints about Internet auction fraud dropped noticeably, according to data released Wednesday, February 7, by the Federal Trade Commission (FTC). More than a quarter of a million ID theft complaints were lodged with the agency last year, accounting for 36 percent of the 674,000 complaints the FTC received. That number is down slightly from 2005, when ID theft accounted for 37 percent of all complaints. This marks the seventh consecutive year that identity theft has been ranked number one. The second−largest number of complaints, seven percent, came from consumers who were unhappy with products they had ordered from catalogs. Internet−related complaints were up too. According to the 2006 data, they made up 60 percent of all fraud complaints. Last year, they accounted for 46 percent. But one area of Internet fraud declined noticeably: Internet auctions.
Source: http://www.infoworld.com/article/07/02/07/HNftcidfraud_1.html?source=rss&url=http://www.infoworld.com/article/07/02/07/H Nftcidfraud_1.html

[Return to top]

Transportation and Border Security Sector

16. *February 08, Government Accountability Office* — **GAO−07−453T: Homeland Security: Observations on the Department of Homeland Security's Acquisition Organization and on the Coast Guard's Deepwater Program (Testimony).** In January 2003, the Government Accountability Office (GAO) designated the Department of Homeland Security's (DHS) implementation and transformation as high risk because of the size and complexity of the effort and the existing challenges faced by the components being merged into the department. The success of the effort to integrate numerous agencies and organizations into one cabinet−level department rests in large part on DHS's ability to effectively acquire the wide range of goods and services it needs to achieve its mission of protecting the nation from terrorism. DHS is undertaking a number of large, complex investments as the federal government increasingly relies on contractors for roles and missions previously performed by government employees. One of the department's largest investments −− the Deepwater program, now estimated to cost $24 billion −− is the Coast Guard's major effort to replace or modernize its aircraft and vessels. Rather than using a traditional acquisition approach, the Coast Guard is using a system integrator to design, construct, deploy, support, and integrate the Deepwater assets. GAO is prepared to discuss (1) the overarching challenges DHS faces in establishing an effective acquisition organization, (2) GAO's prior work on Coast Guard and contractor management of the Deepwater program, and (3) the status of GAO's ongoing reviews.
Highlights: http://www.gao.gov/highlights/d07453thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−453T

17. *February 08, USA TODAY* — **U.S. asks to arm pilots abroad.** For the first time, the U.S. government is asking foreign countries to allow pilots to carry guns in the cockpit when they fly overseas. The Department of Homeland Security, working with the State Department, is trying to expand a four−year−old program that allows thousands of pilots to carry guns on domestic flights. "It's obvious that there's a threat internationally," said Conan Bruce, spokesperson for the Federal Air Marshals Service, which runs the armed−pilots program. "We want to work toward having (armed pilots) be able to perform their duties on international flights." Nations can prohibit armed air marshals on U.S. flights to their countries. Some, including Sweden, have resisted U.S. efforts to have them put their own armed officers on U.S.−bound flights. Thousands of U.S. air marshals fly as passengers on domestic and international flights. The effort to expand the armed−pilots program comes amid criticism that it is falling short of its potential. A Homeland Security report released last month said the program needs improvement, and some policies "may have dissuaded pilots from participating."
Source: http://www.usatoday.com/travel/news/2007−02−07−us−pilots−gun s_x.htm

18. *February 08, Department of Transportation* — **New daily U.S.−China flight awarded to United Airlines.** The Department of Transportation (DOT) on Thursday, February 8, awarded United Airlines the right to operate a daily non−stop flight between Washington Dulles International Airport and Beijing Capital International Airport. This action finalizes DOT's tentative decision to award the seven weekly frequencies to United, whose bid the department

determined would serve the most customers and provide the best service to the traveling public. The Department concluded that selection of United's Washington−Beijing proposal would fill the critical service gap between the Washington, DC metro area and China, and address the increasing demands in the U.S.−China market by providing the greatest increase in capacity. The Department noted that the Washington, DC metro area is the largest city in the proceeding lacking any nonstop service to China.
The final decision, carrier applications, and comments are available on the Internet at http://dms.dot.gov/ docket OST−2006−25275.
Source: http://www.dot.gov/affairs/dot1707.htm

19. *February 08, Associated Press* — **British Airways to charge for extra bags.** British Airways will begin limiting some of its long haul passengers to a single bag per passenger −− and charging them 120 pounds ($236) per flight for every extra piece of luggage each way, the company said Thursday, February 8. The change applies to passengers flying economy class to destinations outside North America, the Caribbean, Nigeria, and Brazil. While passengers to destinations such as Europe and Asia were previously allowed as many bags as they wished, they would now be limited to one bag −− and charged for the excess. Domestic passengers would be charged 30 pounds ($59) for every bag beyond the first, while the price for extra bags taken to Europe would rise to 60 pounds ($118).
Source: http://biz.yahoo.com/ap/070208/britain_british_airways.html?.v=2

20. *February 08, Associated Press* — **FAA issues safety rules for tour firms.** The government announced new safety standards Thursday, February 8, for air tour companies that operate at many scenic vacation spots and for pilots who offer rides at air shows. The Federal Aviation Administration (FAA) also promised to keep closer track of deaths and other accidents involving air tours. Safety investigators have pressed for this, having looked into 107 accidents that killed 98 people between 1998 and 1995. The safety rule, which takes effect in six months, "will increase overall air tour safety, improve the FAA's ability to track and monitor commercial air tour flights and help us identify and address operational trends that could lead to accidents," said the agency's head, Marion Blakey. The FAA's new standards require better passenger briefings and life preservers for passengers on planes that fly over water. Within 18 months, aircraft that fly over water must install floats. The rule also requires air tour companies to get a letter from the FAA permitting them to operate. Companies would have to tell the FAA who runs the operation, who maintains the aircraft, what type of aircraft they use and how their drug and alcohol testing program works.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2007/02/08/AR2007020801166.html

21. *February 08, New York Post* — **Loaded ammo clip found on jet.** A loaded ammo clip was found aboard an American Airlines jet that had just arrived at Kennedy Airport from the Dominican Republic, and police are trying to find its owner. The bullets were discovered in a seat−back pocket on January 29 by a worker cleaning the jet after its flight from Santo Domingo, authorities said on Wednesday, February 7. The plane, which had arrived at Kennedy about two hours earlier, also visited Miami and San Juan, Puerto Rico, that day. But because the jet had been cleaned on its last stop in Santo Domingo, detectives are checking over the manifest from that flight, said a Transportation Security Administration spokesperson. Twenty−six 9mm bullets were loaded into the clip, which a law−enforcement source said was

from a Glock pistol. Like many other carriers, American transports guns and ammunition as checked baggage. Federal rules bar passengers from carrying guns and ammunition aboard.
Source: http://www.nypost.com/seven/02082007/news/regionalnews/ammo_scare_at_jfk_regionalnews_larry_celona_____and_bill_sanderso n.htm

22. *February 07, USA TODAY* — **Airport screeners to get AMBER Alerts.** The nation's 43,000 airport security screeners will get notices and photos of abducted children as part of the AMBER Alert network's quest to find missing people, the Transportation Security Administration (TSA) said Wednesday, February 7. Screeners will be looking to stop abductors from taking children on planes. AMBER alerts are abduction notices sent to authorities and to media outlets, asking for help in locating a missing child. Airports are going to start receiving the bulletins starting today. "This can be tremendously effective," said Ernie Allen, president of the National Center for Missing & Exploited Children, which helps disseminate the alerts. "You're talking about 43,000 TSA officers around the country." TSA screeners check two million people a day at about 450 commercial airports around the USA. "The goal is to get that [alert] to TSA officers within minutes," said Gale Rossides, a TSA associate administrator. Screeners "meet so many children every day, they may actually notice something that's out of character with a child." The TSA effort is the first time AMBER Alerts will go directly to airports, Allen said.
Source: http://www.usatoday.com/news/nation/2007−02−07−amber−alerts_x.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

23. *February 08, Canadian Press* — **Mad cow disease found in Alberta.** Canada has confirmed its ninth case of mad cow disease since 2003, in an Alberta bull. The Canadian Food Inspection Agency said Wednesday, February 7, a mature bull that died on a farm last week tested positive for bovine spongiform encephalopathy (BSE). George Luterbach, the agency's senior veterinarian for Western Canada, said the animal's death caused it to be identified as an "animal of interest" at the farm level as part of a national surveillance program. Provincial and federal tests then confirmed the BSE. Luterbach wouldn't identify where in the province the animal was when it died. An investigation is underway to find other animals born within a year of the bull that may have been exposed to the same feed source, Luterbach said.
Source: http://cnews.canoe.ca/CNEWS/Canada/2007/02/08/3559286.html

24. *February 08, Agricultural Research Service* — **Researchers exploit cattle pathogen's genomic secrets.** With genomic "maps" in hand, Agricultural Research Service (ARS) scientists are plotting new ways to protect cattle from cellular attack by Anaplasmosis marginale. A. marginale is a primarily tick−borne bacterium that invades and destroys the red blood cells of cattle and other ruminant hosts. Severe infections cause anemia, weight loss and

death. Between 50,000 and 100,000 U.S. cattle succumb to it annually. Those surviving the disease—known as anaplasmosis—become lifelong carriers that can endanger other herd members and impede U.S. cattle trade. Although antibiotics can kill A. marginale, a long−sought alternative strategy has been to develop a vaccine to keep the bacterium from infecting cattle in the first place. However, vaccination has been dogged by safety issues and uneven performance. A chief reason is A. marginale's ability to reconfigure its surface proteins and evade detection by the animals' immune systems. Now ARS scientists have had success in determining the nucleic acid sequence for the genome of the bacterium's St. Maries strain, which is tick−transmitted. The advance has enabled the researchers to identify 70 percent of A. marginale's genes, including those encoding for two protein superfamilies. The discovery raises the prospect of devising new vaccines.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

25. *February 08, Los Angeles Times* — **California approves certification program for leafy crops.** California leafy vegetables farmers, still reeling from disease outbreaks linked to their produce, will soon be able to attach seals to their veggies saying their produce is state certified. California agriculture officials on Wednesday, February 7, certified a voluntary food safety program for lettuce, spinach and other leafy vegetables after gaining agreement for the plan from 70 percent of the state's processors and shippers of the greens. The new regulations would create an inspection program to verify that leafy greens handlers are complying with a set of still−to−be established food safety standards. The rules are part of a marketing agreement developed by the leafy greens industry with the help of the California Department of Food and Agriculture. Specific regulations now will be set by the state−appointed board of the marketing agreement and dictate that the shippers purchase produce only from growers who also agree to abide by new farming rules.
Source: http://www.latimes.com/business/la−fi−lettuce8feb08,1,2731830.story?coll=la−headlines−business

26. *February 07, Reno Gazette−Journal (NV)* — **Testing shows no sign of bird flu in Nevada.** The Nevada Department of Wildlife says testing on nearly 2,500 birds throughout Nevada has shown no sign of avian influenza in the state. It was part of a project that detected no cases of the disease anywhere in the Pacific flyway.
Source: http://news.rgj.com/apps/pbcs.dll/article?AID=/20070207/NEWS15/702070474/1144/NEWS

27. *February 07, Express−News (TX)* — **Vineyard disease facing increased scrutiny in Texas.** Texas' burgeoning wine industry is looking to researchers in Fredericksburg to develop controls for a grapevine disease that has troubled wine producers throughout the South. The malady is Pierce's disease, a scourge spread by insects that are native to Texas and abound in the Hill Country. The bacterium, which chokes off the water−conducting capabilities of a vine, is expanding into cooler areas and affects the European−variety grapes that growers would most like to raise. The disease −− considered one of the biggest problems facing California's massive wine industry and which has limited the booming growth of wine−making in Texas −− will undergo closer examination after a research lab is built in Fredericksburg to replace an aging lab that has been conducting studies for two years. The Texas wine industry is the fastest−growing and fifth−largest in the nation. It has 220 vineyards covering 3,700 acres.
Source: http://www.mysanantonio.com/business/stories/MYSA020807.1E.g

rapedisease.1300cfb.html

[Return to top]

Food Sector

28. *February 08, California Aggie* — **University creates new nanoparticles.** Researchers at the University of California, Davis have created a new type of nanoparticle that could be used in tests for environmental pollution and contamination of food products. Nanoparticles are microscopic particles whose size is measured in nanometers or one billionth of a meter. These new nanoparticles have optical and magnetic properties that can be used for biosensors −− devices that use these properties to test samples of food products. The technology has been proven effective in tests to detect bioterrorism agents such as botulinum toxin and ricin in samples of milk, eggs and fruit juice.
Source: http://media.www.californiaaggie.com/media/storage/paper981/news/2007/02/08/ScienceTech/Uc.Davis.Creates.New.Nanoparticles−2706544.shtml?sourcedomain=www.californiaaggie.com&MIIHost=media.collegepublisher.com

29. *February 08, Korea Times* — **Seoul offers U.S. beef concessions.** South Korea on Thursday, February 8, offered a package of concessions to the U.S. in their second day of talks aimed at resolving differences over U.S. beef imports. Korea told U.S. that it could soften quarantine rules on U.S. beef imports, though it maintained its stance to distribute only boneless beef on the market. More specifically, they said that Seoul would reject only boxes of U.S. beef that contain bone fragments and accept bone−free shipments. The U.S. has, however, demanded that Korea import all beef −− boneless or bone−containing −− arguing that it is safe to eat. So far, Korea has rejected all U.S. beef shipments when bone fragments were found. Korea and the U.S. Wednesday, February 7, held the second round of their two−day technical consultations on quarantine inspections of U.S. beef at the National Veterinary Research & Quarantine Service in Anyang, Kyonggi Province.
Source: http://times.hankooki.com/lpage/200702/kt2007020817383353460 .htm

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

30. *February 08, Itar−Tass (Russia)* — **Anti−bird flu measures insufficient.** Russian First Deputy Prime Minister Dmitry Medvedev criticized the measures to combat the spreading of bird flu as inadequate. "The situation is alarming. The measures that are being taken are insufficient," he said at a meeting of the headquarters for coordinating the measures to prevent the spreading of bird flu in the Russian territory.

Source: http://www.itar−tass.com/eng/level2.html?NewsID=11233091&Pag eNum=0

31. *February 08, Food and Agriculture Organization* — **Avian influenza in cats should be closely monitored.** Cats can become infected with the H5N1 avian influenza virus, but at present there is no scientific evidence to suggest that there has been sustained transmission of the virus in cats or from cats to humans, the Food and Agriculture Organization (FAO) said. FAO recommended that in areas where the H5N1 virus has been found in poultry or wild birds, cats should be separated from infected birds until the danger has passed. On commercial poultry premises cats should even be kept indoors. Unconfirmed reports that H5N1 infection has been detected in a high prevalence in cats in Indonesia has caused some alarm. The scavenging cats were sampled in the vicinity of poultry markets in Java and Sumatra where outbreaks of H5N1 avian influenza had recently occurred. This is not the first time that cats have been infected as previous incidents in Thailand, Iraq, the Russian Federation, the European Union and Turkey show. “This raises some concern not only because cats could act as intermediary hosts in the spread of the H5N1 virus between species but also because growth in cats might help the H5N1 virus to adapt into a more highly infectious strain that could spark an influenza pandemic,” said FAO Assistant Director−General Alexander Müller.
Source: http://www.fao.org/newsroom/en/news/2007/1000490/index.html

32. *February 07, World Health Organization* — **Polio in Chad.** On January 23, 2007, the Ministry of Health in Chad confirmed one new polio case. It is the first polio case in Chad since December 2005. A two−year−old girl from N'Djamena had developed paralysis on 26 November 2006. Genetic sequencing of the isolated poliovirus indicates that it is related to poliovirus circulating in northern Nigeria.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.who.int/csr/don/2007_02_07a/en/index.html

33. *February 07, Children's Hospital Boston* — **Discovery could lead to better control of hemorrhagic fever viruses.** Researchers report discovering the receptor through which a group of life−threatening hemorrhagic fever viruses enter and attack the body's cells, and show that infection can be inhibited by blocking this receptor. The findings give a clue to the high lethality of New World arenaviruses, suggest a way of reducing the severity of infection, and point the way toward a needed treatment strategy. The four viruses, known as the Machupo, Guanarito, Junin and Sabia viruses, cause Bolivian, Venezuelan, Argentine and Brazilian hemorrhagic fever, respectively, with mortality rates of about 30 percent. No vaccine is available. In addition to causing occasional disease outbreaks, mostly in poor, rural areas of South America, the viruses are of U.S. government interest because of their potential as bioterrorism agents. All four are classified as Category A Priority Pathogens and must be handled in Biosafety Level 4 containment facilities.
Viral hemorrhagic fevers information:
www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/vhf.htm
Source: http://www.childrenshospital.org/newsroom/Site1339/mainpageS1339P1sublevel281.html

[Return to top]

Government Sector

34. *February 07, Government Accountability Office* — **GAO−07−381R: Homeland Security Grants: Observations on Process DHS Used to Allocate Funds to Selected Urban Areas (Correspondence).** The results of the Urban Areas Security Initiative (UASI) eligibility and funding allocations in fiscal year 2006 raised congressional questions and concerns about Department of Homeland Security's (DHS) methods in making UASI determinations. Several congressional members requested that the Government Accountability Office (GAO) examine aspects of DHS's UASI funding process, and the fiscal year 2007 DHS Appropriations Act directed GAO to examine the validity, relevance, reliability, timeliness, and availability of the risk factors (including threat, vulnerability, and consequence) used by the Secretary of Homeland Security for the purpose of allocating discretionary grants. On November 17, 2006, GAO responded to the mandate and the request by briefing congressional staff on the results of this review. GAO specifically examined (1) DHS's method of estimating relative risk of terrorism in fiscal year 2006; (2) DHS's process for assessing the effectiveness of the various risk mitigation investments submitted in UASI applications; (3) how DHS used estimated relative risk scores and assessments of effectiveness to allocate UASI grant funds in fiscal year 2006; and (4) what changes, if any, DHS plans to make in its UASI award determination process for fiscal year 2007. This letter and the accompanying appendices transmit the information provided during those briefings.
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−381R

[Return to top]

Emergency Services Sector

35. *February 07, Government Technology* — **New public safety headquarters in Atlanta breaks ground.** The City of Atlanta, GA, recently broke ground on a joint police and fire headquarters that will become a best−in−class public safety and judicial services center. The new headquarters will serve as a joint administrative hub for the Atlanta Police Department and the Atlanta Fire Rescue Department. In addition to housing police, fire and rescue personnel, the new headquarters will include a joint operations center and media room for police and fire personnel, armory, and a fitness center.
Source: http://www.govtech.net/news/news.php?id=103823

36. *February 07, Federal Emergency Management Agency* — **DHS establishing a National Advisory Council.** The Department of Homeland Security (DHS) announced Wednesday, February 7, the establishment of the National Advisory Council, which is being created to advise the Administrator of the Federal Emergency Management Agency (FEMA) on all aspects of emergency management in an effort to ensure close coordination with all involved. "The development of the National Advisory Council, along with the tireless efforts of the dedicated public servants at FEMA, will go hand−in−hand in setting the course to obtain our vision for a new FEMA," said FEMA Director David Paulison. "Together, we will lead our organization to become the Nation's Preeminent Emergency Management Agency." Members of the Council will be appointed by the Administrator of FEMA, and will represent a geographic and significant cross section of officials from emergency management and law enforcement, and include homeland security directors, adjutants general, emergency response providers from state, local, and tribal governments, private sector, and nongovernmental

organizations. The Council is being instituted to ensure effective and ongoing coordination of the federal preparedness, protection, response, recovery and mitigation for natural disasters, acts of terrorism, and other man−made disasters.
Source: http://www.fema.gov/news/newsrelease.fema?id=33888

[Return to top]

Information Technology and Telecommunications Sector

37. *February 08, eWeek* — **Botnet stalkers share takedown tactics at RSA.** A pair of security researchers speaking at the ongoing RSA Conference Wednesday, February 7, demonstrated their techniques for catching botnet operators who use secret legions of infected computers to distribute malware programs and violent political propaganda. The botnet experts, both of whom are employed by anti−malware software maker FaceTime Communications, detailed how they identified and pursued individuals believed to be responsible for running a pair of sophisticated botnet schemes, which have been subsequently shut down or significantly scaled back. Addressing a packed room of conference attendees, Chris Boyd and Wayne Porter offered a rare inside glimpse into the world of botnet herders, which the researchers entered by hanging out on the shady online bulletin boards and chat relays where the schemers meet to share the tricks of the trade and their malware programs. By luring the prolific scammers to offer details about their work, and spying on the criminals, the researchers claim to have pieced together the identities of several of the unsavory individuals and helped take down their networks of subverted machines.
Source: http://www.eweek.com/article2/0,1895,2092435,00.asp

38. *February 08, Information Week* — **Polycom boosts Wi−Fi voice effort with SpectraLink acquisition.** Polycom reported that it will acquire SpectraLink for $220 million in cash in a move that will bolster Polycom's drive into the nascent voice over Wi−Fi market. The addition of SpectraLink will boost Polycom's ability to provide fixed and mobile telecommunications products covering voice, video, and data over desktop and mobile environments.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=4MG1IA020SCFCQSNDLOSKH0CJUNN2JVN?articleID=197004389

39. *February 08, SecurityFocus* — **US−CERT: Companies increasingly reporting attacks.** Corporate America is getting better about telling the U.S. government about serious security incidents, according to an official from the Department of Homeland Security (DHS). In 2006, companies, universities and government agencies reported 23,000 incidents to the U.S. Computer Emergency Readiness Team (US−CERT), up from 5,000 reported in 2005, Jerry Dixon, deputy director of the DHS's National Cyber Security Division, said at the RSA Security Conference on Wednesday, February 7. So far, in the first quarter of 2007, more than 19,000 incidents have been reported to US−CERT, Dixon said. "Increasingly, the private sector is reporting these incidents," Dixon said. "We are getting a much better picture than what we use to get at the DHS."
Source: http://www.securityfocus.com/brief/430

40. *February 07, eWeek* — **Symantec spots exploit for Excel zero−day flaw.** Symantec has

uncovered malicious code that could exploit Microsoft's newest zero−day vulnerability. Wednesday, February 7, on Security Response Weblog, Symantec revealed the exploit, which could drop a back−door Trojan onto an infected system. The exploit "may enable an attacker to gain remote access to your computer," wrote Amado Hidalgo in the blog post. The malicious code "appears to be exploiting a bug on MSO.DLL," which is an Office shared library, Hidalgo wrote. In a security bulletin issued on February 2, Microsoft warned that "other Office applications are potentially vulnerable" to the zero−day flaw. Symantec has only seen code that exploits Excel. The exploit actually uses two different Trojans. The first, Trojan.Mdropper.Y, drops the second, Backdoor.Bias. Symantec has released patches for both Trojans. A signature update for the first one was issued Wednesday. "Fully patched versions of Office 2000, XP and 2003 appear to be vulnerable to this exploit," Hidalgo wrote.
Symantec blog: http://www.symantec.com/enterprise/security_response/weblog/2007/02/latest_office_zeroday_vulnerab.html
Source: http://www.eweek.com/article2/0,1895,2091695,00.asp

41. *February 07, CNET News* — **Two flaws found in Firefox.** A security company has reported two new flaws in the Mozilla Firefox browser that may leave locally saved files vulnerable to outside attacks. Both flaws were announced by SecuriTeam, a division of Beyond Security, this week. The first flaw lies in Firefox's pop−up blocker feature, according to a SecuriTeam statement on Monday, February 5. The browser typically does not allow Websites to access files that are stored locally, according to the official report, but this URL permission check is superseded when a Firefox user has turned off pop−up windows manually. As a result, an attacker could use this flaw to steal locally stored files and personal information that might be stored in them. The second flaw, announced by SecuriTeam on Wednesday, concerns Firefox's phishing protection feature. With this vulnerability, an adept phisher could fool the browser into believing that a fraudulent site is actually secure by adding particular characters into the URL of its Website. The phishing flaw does appear to apply to the current 2.0.0.1 version of Firefox.
Popup blocker flaw advisory: http://www.securiteam.com/securitynews/5JP051FKKE.html
Phishing flaw advisory: http://www.securiteam.com/securitynews/5MP0320KKK.html
Source: http://news.com.com/Two+flaws+found+in+Firefox/2100−1002_3−6 157307.html

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: 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

42. *February 08, Boston Globe* — **Massachusetts town faces $400,000 in levee repairs.** The federal government has declared that a levee that diverts part of the Canton River around the Plymouth Rubber Co. in Canton, MA, is one of 146 dams and levees in the nation that are in need of immediate repair. The move surprised residents and town officials, who say repairs will

cost the town about $400,000 in an already cash−strapped year. Although the levee was found to be in "fair" repair in October, the Army Corps of Engineers said last week that −− under tightened federal regulations put in place after Hurricane Katrina −− it is now considered "structurally deficient." The Army Corps set a one−year deadline for the town to fix it. Officials from the Federal Emergency Management Agency will meet soon with town officials to determine which properties might be at greater risk of flooding given the new classification of the levee. Victor D. Del Vecchio, chairman of the Board of Selectmen, said repairs have been estimated at $400,000 and that the money will likely be included in the town budget that will go before the annual Town Meeting on April 30.
Source: http://www.boston.com/news/local/articles/2007/02/08/town_faces_400000_in_levee_repairs_1_year_deadline_set/

43. *February 07, Associated Press* — **Three pipe bombs found in California aqueduct.** Three pipe bombs were found near a valve in a portion of the California Aqueduct near Pearblossom that was partially drained to check for submerged objects, officials said. The bombs were among numerous items found Tuesday, February 7, during an inspection, which also yielded 25 vehicles and at least four weapons, California Highway Patrol Sgt. Fernando Contreras said. "The pipe bombs were found by a check valve, so we don't know if those were left there intentionally," he said. "If the bombs went off, it could release the valve and open it and release water." Pearblossom is in the eastern Antelope Valley along the east branch of the California Aqueduct, which carries water from the northern part of the state to Southern California.
Source: http://www.dailynews.com/news/ci_5180780

[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