Department of Homeland Security Daily Open Source Infrastructure Report for 12 February 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- The Guardian reports that the U.S. is pressing the 27 governments of the European Union to sign up for a range of new security measures for transatlantic travel, including allowing armed guards on all transatlantic flights by U.S. airlines. The new American demands go well beyond what is agreed under the existing U.S.-EU Passenger Name Record Agreement. Brussels is pressing European governments not to sign bilateral deals with the U.S. to avoid weakening the EU bargaining position. (See item **14**)
- According to Computer Weekly, research by security software house McAfee shows that mobile phone users are increasingly worried that PC-based information security risks are threatening their phones. A security analyst at McAfee said 58 percent of respondents worried about spam, fraudulent use of subscribed services, and theft of data stored on their phones. (See item **36**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *February 11, Associated Press* – (Virginia) **Winds fuel wildfire, thousands without power.** Thousands of Virginians were without power Monday morning as crews across the state battled wildfires fueled by dry conditions and fanned by gusty winds. Virginia's governor declared a state of emergency on Sunday and activated the Virginia

National Guard to be available to help battle wildfires caused by high winds knocking out power lines. Some homes were evacuated. Dominion Virginia Power reported on its Web site that about 27,000 Virginia homes and businesses were still without electricity Monday morning.
Source:
http://www.delmarvanow.com/apps/pbcs.dll/article?AID=/20080211/WCT01/80211008/1052/CB

2. *February 10, Associated Press* – (National; International) **Chavez threatens U.S. oil cutoff.** Venezuelan President Hugo Chavez on Sunday threatened to cut off oil sales to the U.S. in an "economic war" if Exxon Mobil Corp. wins court judgments to seize billions of dollars in Venezuelan assets. Exxon Mobil has gone after the assets of state oil company Petroleos de Venezuela SA in U.S., British, and Dutch courts as it challenges the nationalization of a multibillion dollar oil project by Chavez's government. A British court has issued an injunction "freezing" as much as $12 billion in assets. Chavez has repeatedly threatened to cut off oil shipments to the U.S., which is Venezuela's primary client, if Washington tries to oust him. Chavez's warnings on Sunday appeared to extend that threat to attempts by oil companies to challenge his government's nationalization drive through lawsuits. "If you end up freezing (Venezuelan assets) and it harms us, we're going to harm you," Chavez said during his weekly radio and television program. "Do you know how? We aren't going to send oil to the United States." Venezuela accounted for about 12 percent of U.S. crude oil imports in November, the latest figures available from the U.S. Energy Department, making Venezuela the U.S.'s fourth-biggest oil importer.
Source: http://www.breitbart.com/article.php?id=D8UNOD3G0&show_article=1

3. *February 8, KSBY 6 Santa Barbara* – (California) **Greka announces oil spills were caused by someone with inside knowledge.** A Greka Oil security consultant says he has strong indications two of the company's spills in Santa Barbara County, California, were no accident. On Friday, the consultant announced that the spills that occurred on December 7 and January 4 were caused by someone with inside knowledge of the oil industry. Stop work orders were placed at several Greka sites following numerous oil spills during the past couple months. Greka says the investigation into alleged sabotage will continue.
Source: http://www.ksby.com/Global/story.asp?S=7846693

[Return to top]

Chemical Industry Sector

4. *February 11, Beaumont Enterprise* – (Texas) **Region's plants stress safety.** It is three times safer to work at a petrochemical plant in Southeast Texas than in a grocery store, according to the Southeast Texas Plant Managers Forum. Locals believe refinery and chemical plants in Southeast Texas share a culture of safety not apparent at the BP refinery in Texas City. In the past ten years, plants here have suffered at least eight fires, including an explosion in April 2006 at Huntsman Chemical Co. that burned for days. But those incidents resulted in a few injuries and no deaths. Industry officials point to

heavy investment in safety personnel, regular equipment upgrades, stringent training requirements, and regular testing of plant emergency warning systems as the reasons accidents in Southeast Texas do not escalate to the level of disasters like BP's. In the past decade, the Beaumont Enterprise reported two deaths at petrochemical plants, neither of which was caused by the types of hazardous conditions investigators determined were present at BP's refinery before the March 23, 2005, disaster. "Texas, I think, merits better than the national average and we're very proud the chemical industry is two times as safe as the manufacturing industry," said the president of the Texas Chemical Council.
Source:
http://www.southeasttexaslive.com/site/news.cfm?newsid=19280655&BRD=2287&PAG=461&dept_id=512588&rfi=6

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *February 11, WIS 10 Columbia* – (National) **NRC seeks public comment on plan to import Italian nuclear waste.** The Nuclear Regulatory Commission is seeking public comment on a plan to import about 20,000 tons of nuclear waste from Italy for processing in Tennessee and disposal in Utah. The regulatory agency published notice in the Federal Register on Monday that it was allowing 30 days for petitioners to seek a hearing or request to become an intervener on the plan sought by Utah-based EnergySolutions Inc. The company would bring in the waste – mostly paper, plastic, wood, metal, and ion-exchange resins from shuttered nuclear plants – through the ports of Charleston, South Carolina, or New Orleans, Louisiana.
Source: http://www.wistv.com/Global/story.asp?S=7853621

6. *February 11, Associated Press* – (New Jersey) **Some radiation detectors at Oyster Creek nuclear plant are down.** Radiation might be harder to detect at the Oyster Creek nuclear power plant in Lacey Township, New Jersey. Five of 19 devices that monitor radiation on and near the plant were down last week. State Environmental Protection Department officials say enough monitors are working so that a leak would be discovered quickly. Officials hope a new computer system expected to be in place by summer will end some of the glitches with the monitors.
Source: http://www.pressofatlanticcity.com/news/newjersey/story/7534860p-7437627c.html

7. *February 10, Laboratory News* – (International) **Nuclear power under scrutiny.** The University of Manchester will lead a three-year project to develop a methodology and decision-support system for assessing the sustainability of nuclear power, considering both energy supply and demand. "The Sustainability Assessment of Nuclear Power: An Integrated Approach" project is being led by a professor in the School of Chemical Engineering and Analytical Science. The framework being developed will draw together technical, environmental, economic, social, and governance perspectives to enable systematic, transparent, and balanced assessment of nuclear power relative to other energy options – including renewables.

Source: http://www.labnews.co.uk/laboratory_article.php/2985/2/2/nuclear-power-under-scrutiny

[Return to top]

Defense Industrial Base Sector

8. *February 11, Washington Technology* – (National) **CSC to support Air Force pilot training.** Computer Sciences Corp. (CSC) will provide technical support services to the Air Force's Air Education and Training Command under a six and a half year contract that could be worth as much as $482 million. Under terms of the award, CSC will provide aircraft maintenance and base operating services that support the mission requirements of the 71st Flying Training Wing at Vance Air Force Base, Enid, Oklahoma.
   Source: http://www.washingtontechnology.com/online/1_1/32250-1.html?topic=contract-awards

9. *February 11, Washington Times* – (National) **Several arrested in Chinese spy sweep.** On Monday, the FBI arrested a Pentagon official and two Chinese-born residents on espionage charges for passing defense secrets to China, the Justice Department announced. A resident of Alexandria, Virginia, was arrested at his home on espionage charges. He worked as a weapons system analyst for the Defense Security Cooperation Agency, in Arlington, Virginia, which is in charge of U.S. arms sales to foreign nations. He held a top-secret clearance. One official said the case involved the transfer of command, control, communications, and intelligence equipment originally sold to Taiwan that was diverted to China. A Taiwan-born U.S. citizen and a Chinese national, both from New Orleans, were arrested in New Orleans on charges of conspiracy to provide defense secrets to China. Court papers state that the three men conspired to transfer defense secrets during meetings with Chinese intelligence officials. Meanwhile, a naturalized U.S. citizen and former Boeing engineer was arrested this morning after being indicted last week on charges of economic espionage and acting as an unregistered Chinese agent. The man, a Rockwell International engineer until the company was bought by Boeing in 1996, held a top-secret clearance. He was arrested at his home in Orange, California. He was indicted Wednesday on eight counts of economic espionage, one count of conspiracy to commit economic espionage, one count of acting as an unregistered foreign agent, one count of obstruction of justice, and three counts of making false statements to FBI investigators. The case is expected to lead to a further curtailing of U.S.-China space cooperation, which was halted temporarily last year after China carried out an anti-satellite weapon test that left thousands of pieces of debris in low Earth orbit.
   Source:
   http://www.washingtontimes.com/apps/pbcs.dll/article?AID=/20080211/NATION/718249348/1001

[Return to top]

Banking and Finance Sector

10. *February 11, New York Daily News* – (National) **Craigslist scams targeting renters desperate for affordable apartments.** An Internet fraud and security expert warned apartment seekers of scams meant to profit from gullible people desperate for affordable housing. "It is becoming more common because New York apartments have become such a hot commodity," he said. "People are so desperate that they aren't always thinking clearly." For example, a fully furnished two-bedroom with a balcony in Bay Ridge, Brooklyn, going for $950 instead of the $2,200 it would normally fetch because of the tenant's sudden job transfer. The catch: You have to take it sight unseen – and send a security deposit. According to the expert, "countless" victims fell for this scam, sent money, and never heard back from the renters. "Craigslist is made to sell local, and whenever anyone from out of state is involved, red flags should immediately go up," he said. "Avoiding the scam is simple. Try to always do business face-to-face, and never, ever, wire money anywhere." This is also the advice posted under "avoiding scams and fraud" by Craigslist on its Web site, which urges users not to wire money, give out personal financial information, or respond to any offers requiring people to provide escrow money. "Know that only a scammer will 'guarantee' your transaction," Craigslist warns. "People need to remember that if it sounds too good to be true, it probably is."
    Source: http://www.nydailynews.com/news/2008/02/11/2008-02-11_craigslist_scams_targeting_renters_despe-2.html

11. *February 11, KTAR 92.3 Phoenix* – (Arizona) **AG's office warns about identity theft scams.** Some brazen new scams have appeared in Arizona, prompting the attorney general (AG) to warn people to be careful. He says identity thieves have been calling people, representing themselves as a reputable bank or organization – or in some cases claiming to be from his office. "They claimed they were from our office and they had a consumer settlement and they wanted information so they could send a check," the AG said. "Many people, unfortunately, believed them and gave them that information." "Seniors, especially, have been victimized by some of these basic efforts to try to get their financial information by any way, hook or crook..." "The attorney general's office, the Internal Revenue Service, any government institution will never call you cold and say, 'I want to have your name and Social Security number,'" he said. One of the big scams right now involves callers claiming to be with the IRS, and saying people are eligible for an advance on their tax return if they pass on their bank account number.
    Source: http://ktar.com/?nid=6&sid=729168

12. *February 11, Canadian Press* – (National) **Identity thieves turn to old-fashioned mail and telephones.** When it comes to identity theft, most people think they are especially vulnerable when they are working on their computers, or when fraudsters hack into big databases and steal card numbers. In fact, consumers are far more likely to be victimized if their wallet, checkbook, or credit card is lost or stolen, said a new study released Monday by Javelin Strategy & Research. The research group, which is based in San Francisco, also found as financial institutions and retailers have improved their in-store and online security, ID thieves have turned to more-traditional channels of theft,

especially the telephones and the mail. While the incidence of ID fraud through in-store and online purchases declined in the latest survey, conducted last October, from a similar study in 2006, the portion of fraud stemming from mail or telephone purchases jumped to 40 percent from three percent. While the Javelin study found overall ID theft is falling, it also found the cost for consumers to resolve the resulting fraud is rising. The latest study indicated 8.1 million Americans were victims of ID fraud in 2007, down from 8.4 million a year earlier and 10.1 million in 2003. The total cost of ID fraud also dropped, to $45 billion in the latest study from $51 billion a year earlier and $56 billion in 2003. But the average cost for a consumer to resolve the problem rose to $691 in 2007 from $554 a year earlier. The biggest sources of personal identification information for thieves included: 33 percent from the loss or theft of a wallet, check, or credit card; 23 percent from in-store, mail, or telephone purchases; 17 percent from misappropriation of information by friends, relatives, or in-home employees; eight percent from computer viruses, spyware, or hackers; seven percent from data breaches, and six percent from stolen paper mail. Also ironically, fraudsters often take the information they steal from individuals and use it to open wireless phone accounts, he added. "Phone accounts are the No. 1 new account being opened," Javelin's president said.
Source: http://canadianpress.google.com/article/ALeqM5gri6492jGw5-lk6gIwbdi6yUHIqQ

13. *February 11, Quad-City Times* – (Illinois) **Phishing scam uses threat.** A new Internet scam had Moline, Illinois, police investigating death threats delivered to two Moline residents by e-mail this week. Police confirmed the e-mails were an Internet phishing scam and not a real threat. Police investigated the threats and found they originated from Mexico and Israel but were almost identical and resembled a generic form letter, said a police official. The e-mails contained the heading: "BE MORE CAREFUL." The sender claims they have been paid to kill the e-mail recipient and have the victim's name, picture, and other information, but does not give specifics. They also claim they are watching the victim. They try to negotiate with the e-mail recipient on "fees" to spare their life and offer to sell a tape recording of the murder for hire solicitation. It also warns the victim not to contact police. The sender's goal is to extort private information such as credit card and bank information, he said. "There is a possibility there is more," he said of the e-mails. "A lot of people will take it as spam or phishing and not notify us, which is fine." The police official said they do not pursue the investigation once its determined the threat originated from a foreign country. He advised those who receive such e-mails to visit the FBI's Crime Complaint Center at ic3.gov and report the incident. He said the FBI is overwhelmed with similar reports of phishing and has set up the Web site to collect reports.
Source: http://www.qctimes.com/articles/2008/02/11/news/local/doc47ad407e11607276135313.txt

[Return to top]

Transportation Sector

14. *February 11, Guardian* – (International) **Bush orders clampdown on flights to U.S.** The U.S. administration is pressing the 27 governments of the European Union (EU) to sign up for a range of new security measures for transatlantic travel, including allowing armed guards on all flights from Europe to America by U.S. airlines. According to a U.S. document being circulated for signature in European capitals, EU states would also need to supply personal data on all air passengers overflying, but not landing in the U.S., in order to gain or retain visa-free travel to America, senior EU officials said. And within months, the U.S. Department of Homeland Security is to impose a new permit system for Europeans flying to the U.S., compelling all travelers to apply online for permission to enter the country before booking or buying a ticket, a procedure that will take several days. The data from the U.S.'s new electronic transport authorization system is to be combined with extensive personal passenger details already being provided by EU countries to the U.S. for the "profiling" of potential terrorists and assessment of other security risks. Washington is also asking European airlines to provide personal data on non-travelers – for example family members – who are allowed beyond departure barriers to help elderly, young, or ill passengers to board aircraft flying to America, a demand the airlines reject as "absurd." Seven demands tabled by Washington are contained in a 10-page "memorandum of understanding" that the U.S. authorities are negotiating or planning to negotiate with all EU governments, according to ministers and diplomats from EU member states and senior officials in Brussels. The Americans have launched their security drive with some of the 12 mainly east European EU countries whose citizens still need visas to enter the U.S. As part of a controversial passenger data exchange program allegedly aimed at combating terrorism, the EU has for the past few months been supplying the American authorities with 19 items of information on every traveler flying from the EU to the U.S. The new American demands go well beyond what was agreed under that Passenger Name Record system and look certain to cause disputes within Europe and between Europe and the U.S. Brussels is pressing European governments not to sign the bilateral deals with the Americans to avoid weakening the EU bargaining position.
Source: http://www.guardian.co.uk/world/2008/feb/11/usa.theairlineindustry

15. *February 10, East Valley Tribune* – (Arizona) **Phoenix airport secures 'prohibited item'.** Officials said about 600 passengers were re-screened on Sunday after a suspicious item was found at Phoenix's main airport. The undisclosed "prohibited item" was found near the checkpoint of Terminal 2 of Phoenix Sky Harbor International Airport around noon, according to airport officials. Six flights were delayed as a result of the re-screening. "There was not any eminent danger," said a Transportation Security Administration spokeswoman. She said the re-screening was done as a precaution.
Source: http://www.eastvalleytribune.com/story/108694

16. *February 10, News 13 Orlando* – (Florida) **Suspicious device sends bomb squad to port.** In Florida, the Brevard County Bomb Squad was called in to Port Canaveral Saturday after a suspicious device was reported. It was near the Carnival Glory at Terminal 10. The incident happened as passengers were showing up for their cruise. Officials said the object turned out to be a piece of luggage. The sheriff's office said port operations were interrupted until the owner was found. The luggage did not have to be

destroyed. Two cruise ships were at the port at the time -- The Carnival Glory and Disney Magic.
Source:
http://www.cfnews13.com/News/Local/2008/2/9/suspicious_device_sends_bomb_squad_to_port.html

17. *February 9, Bay Area News* – (California) **Worker at SFO held on gun charge.** A United Airlines employee at San Francisco International Airport was arrested Thursday on suspicion of sneaking a loaded handgun into a secure area of the airport, authorities said Friday. The employee reportedly had a dispute with colleagues at work and someone discovered during the argument that the person had a firearm, an FBI Special Agent said. A spokeswoman for the San Mateo County Sheriff's Office said the worker was charged on suspicion of one count of possessing a concealed weapon and one count of possessing a loaded gun. Federal agents responded to the incident because bringing a weapon into a secure area of an airport is a federal crime. The suspect will not face federal charges, added the FBI official.
Source: http://www.insidebayarea.com/sanmateocountytimes/ci_8216493

18. *February 9, News-Press* – (Florida) **3 arrested after trying to climb airport fence.** Three men are in custody in Lee County, Florida, after they were caught trying to climb a fence at Southwest Florida International Airport. The three men were spotted in a car near the Hertz rental car counter at the airport, according to a Lee County Port Authority spokeswoman. A Hertz representative called them in as suspicious persons, but when law enforcement arrived, they found the men had abandoned the car. The three were found attempting to climb a fence and arrested.
Source: http://www.news-press.com/apps/pbcs.dll/article?AID=/20080209/NEWS01/80209033/1002

[Return to top]

Postal and Shipping Sector

19. *February 11, Chatham Daily News* – (International) **Powder causes alarm; suspicious substance deemed harmless.** The Chatham-Kent Police Service headquarters in Ontario, Canada, was briefly quarantined Saturday afternoon after two concerned citizens brought in a suspicious substance. However, officials have since deemed the white, crumbly material harmless. A staff sergeant told the Chatham Daily News the pair opened an envelope, which was not addressed to them, and discovered the substance. He said police took standard precautions given the situation. "We contained the lobby," he said. "The substance wasn't something that could become airborne." The envelope was postmarked from Chicago and featured writing in a foreign language. A joint investigation with the FBI's Chicago office later indicated the mail originated from an elderly woman of Polish descent. Police said the investigation is complete pending a confirmation analysis of the product. The staff sergeant advised people never to open strange mail, saying it should simply be returned to the sender. However, he said if they do open it, to contact police when any suspicious material is found and leave the envelope or package where it is. "Don't bring it into the police station," he said.

Source: http://www.chathamdailynews.ca/ArticleDisplay.aspx?e=897400

20. *February 10, WKRC 12 Cincinnati* – (Ohio) **Suspicious powder found in bank envelope.** Cincinnati firefighters were called late Saturday morning to a U.S. Bank facility that processes envelopes. As a machine was opening an envelope, a powdery substance shot out. It went into the air and also left residue on the machine. No one was hurt, but firefighters are trying to determine whether or not the powder is toxic. The building was also vented as a precaution.
Source: http://www.local12.com/news/local/story.aspx?content_id=4048a34b-5fe9-4930-93c9-8c6fa9dc3650

21. *February 9, West Central Tribune* – (Wisconsin) **Appleton inmate is charged for threat to the IRS.** An inmate at the Prairie Correctional Facility in Appleton is alleged to have attempted an anthrax hoax against the Internal Revenue Service. A federal grand jury indicted a prisoner at the Prairie Correctional Facility, on Thursday for mailing an envelope containing a white powder purporting to be anthrax to an IRS facility in Kansas City, Missouri. He is charged with engaging in conduct with the intent to convey false or misleading information regarding a biological weapon, according to a news release from the U.S. Attorney Western District of Missouri. Authorities are aware of the man's current status as an inmate and consequently have not taken action to bring him into federal custody, according to a public affairs director with the U.S. Attorney's office. He will be transferred to Kansas City for an appearance on the charge at a date yet to be determined, he added.
Source: http://www.wctrib.com/articles/index.cfm?id=31540&section=News

[Return to top]

Agriculture and Food Sector

22. *February 11, Associated Press* – (Texas) **Texas cotton prospects dimming.** The South Plains region of Texas has gone 60 days without significant rain; humidity has been low; and windy conditions have prevailed since early January. It is still about ten weeks until farmers start planting in the world's largest contiguous cotton patch; but the arid, windy conditions are sucking moisture on the soil's surface, damaging the subsurface moisture that newly planted cottonseed needs to germinate and grow. Last year, heavy rainfall throughout Texas – the nation's leading cotton-producing state – led to the second-largest crop on record last year: 8.1 million bales, 5.3 million from the South Plains. Dry conditions are worse for dryland cotton producers, who rely on rainfall only to grow the plants. But switching to other crops such as corn does not make much sense because those crops would need more water. With a strong La Nina influencing weather patterns, the chance of heavy rain is not good, weather officials said. The last significant rainfall came December 11; dew points have dipped below zero; and humidity has reached single digits.
Source:
http://ap.google.com/article/ALeqM5icEiT6msrz46LoAfs2hLcEk7E7WQD8UO0ER00

23. *February 11, Voice of America* – (National) **Study shows growing biofuel crops costly**

to environment. Converting land to grow biofuel crops as cleaner-burning alternatives to fossil fuels actually results in major new carbon emissions, according to a new study published in the online edition of the journal Science. The study's author, a regional director with the Nature Conservancy, says clearing forests, grass, and peatlands to make way for biofuel crops like corn and soybeans causes the carbon naturally stored in the soil to escape into the atmosphere. The study cites prime locations where this is already taking place: The grasslands of the American Midwest, the rainforests and savannahs of Brazil, and the peatlands of Southeast Asia. New fuel standards in the U.S. mandate that biofuel production reach 136.3 billion liters by 2022. According to the study, that would require the cultivation of 24.3 million hectares of farmland, or twice the area of Pennsylvania. Yet it would supply only ten percent of the energy needed to meet the nation's transportation demands.
Source: http://www.voanews.com/english/Science/2008-02-11-voa13.cfm

24. *February 10, USA Today* – (National) **Trader Joe's to exclude some food imports from China.** Trader Joe's grocery stores are dropping foods from China to satisfy customers concerned about the quality of that country's products after last year's spate of problems. By April 1, Trader Joe's will phase out single-ingredient Chinese imports such as garlic, frozen organic spinach, ginger, and edamame, a spokeswoman said. The ban does not include products with ingredients from China, a leading source of vitamins and minerals used in many processed foods. With 285 stores in 23 states, Trader Joe's is known for good prices on a wide selection of exotic items. Federal regulators last year warned about contaminated Chinese pet food ingredients, fish containing antibiotics not allowed in human food, and toothpaste laced with a chemical used in antifreeze. Trader Joe's stance is not likely to be widely copied. Major grocers depend on a global market to meet consumer demands for variety. Instead of relying upon blanket bans, retailers say they must choose product sources carefully and check that safety standards are met. China is a leading exporter of garlic, apple juice, and seafood, but probably supplies less than one percent of the U.S.'s food, says the Agriculture Department. Still, China's products show up often in food recalls, Food and Drug Administration (FDA) data show. Of the 14 food recalls tracked by the FDA since December 1, four of the eight identified as imports were from China. Products from India, Mexico, Turkey, and the U.S. were also recalled, indicating that any country can face food-safety challenges.
Source: http://www.usatoday.com/money/industries/food/2008-02-10-trader-joes-china_N.htm

[Return to top]

Water Sector

25. *February 10, Canadian Press* – (International) **Canadian judge to rule on Mexican water fight.** More than 40 Texas farmers, ranchers, and irrigation districts are gearing up to take their long-standing water war with Mexico to the next level, which in this case is a Canadian judge. The farmers sued Mexico in 2004 for $500 million, arguing they had been shorted on Rio Grande River water from 1992 to 2002 in violation of a 1944 treaty. In June, a tribunal operating under the North American Free Trade Agreement decided it had no jurisdiction to hear the case in which Washington sided

with Mexico. The groups now plan to ask a Canadian judge – considered a neutral arbitrator – on March 25 whether the tribunal erred and deprived them of a fair hearing.
Source:
http://canadianpress.google.com/article/ALeqM5gM5AYhvZj90WTIRWosjnOM1VZcOw

26. *February 9, Associated Press* – (National) **Judges overturn EPA's mercury plan.** A federal appeals court said Friday the current presidential administration ignored the law when it imposed less-stringent requirements on power plants to reduce mercury pollution, which scientists fear could cause neurological problems in 60,000 newborns a year. A three-judge panel unanimously struck down a mercury-control plan imposed by the Environmental Protection Agency (EPA) three years ago. The agency established an emissions-trading process in which some plants could avoid installing the best mercury-control technology available by buying pollution credits. Environmentalist and health experts said such a cap-and-trading mechanism would create "hot spots" of mercury contamination near some power plants. Seventeen states and environmental and health groups joined in a suit to block the regulation, saying it did not adequately protect public health. Power plants are the biggest source of releases of mercury, which ends up in the food supply, particularly fish.
Source:
http://seattletimes.nwsource.com/html/nationworld/2004173335_mercury09.html?syndication=rss

[Return to top]

Public Health and Healthcare Sector

27. *February 11, New York Times* – (National) **Scientists find new receptor for H.I.V.** Government scientists have discovered a new way that H.I.V. attacks human cells, an advance that could provide fresh avenues for the development of additional therapies to stop AIDS, they reported on Sunday. The discovery is the identification of a new human receptor for H.I.V. The receptor helps guide the virus to the stomach after it gains entry to the body, where it begins its relentless attack on the immune system. The findings were reported online Sunday in the journal Nature Immunology by a team headed by the director of the National Institute of Allergy and Infectious Diseases.
Source: http://www.nytimes.com/2008/02/11/health/11aids.html?ref=us

28. *February 11, Fox News* – (New York; National) **Two children in New York State die from influenza, is an outbreak headed to your city?** Two children died from influenza in upstate New York in the past two weeks, just as 11 states reported widespread flu activity across the U.S. The two tested positive for the influenza A and influenza B strains of the virus. Although this debilitating seasonal scourge usually peaks in mid-February, this year health officials are already on alert. The complications seen in recent years, such as the rise in pediatric flu deaths with bacterial infections, have been compounded by concerns of a drug-resistant strain that has cropped up in various countries. All of the drug-resistant viruses are found within the H1N1 strain, one of the three main types of influenza affecting humans this year. Of those strains, 6.7

percent have been found to be resistant to Tamiflu (oseltamivir), an antiviral medication that has been shown to shorten the duration of the flu when taken within two days of infection. Although some health experts say it is too early to tell whether this flu season will follow in the footsteps of last year's mild outbreak, some clinicians are already seeing more cases.
Source: http://www.foxnews.com/story/0,2933,330309,00.html

29. *February 10, USA TODAY* – (National) **Off-label Botox use linked to serious side effects.** Botulinum toxin (Botox) injections, best known for smoothing wrinkles, have been linked to cases of serious reactions, including death, the Food and Drug Administration (FDA) announced Friday. The FDA has received at least one report of a patient hospitalized after getting injections for cosmetic purposes, but it was "unlikely" that the drug was to blame, the director of the neurology products division at the FDA's Center for Drug Evaluation and Research told reporters. Most of the severe reactions that occurred in children treated for limb spasticity were associated with cerebral palsy, an off-label use. Such off-label uses are appropriate if the physician believes they are, the director said.
Source: http://www.usatoday.com/news/health/2008-02-10-botox-side-effects_N.htm

Government Facilities Sector

30. *February 10, Associated Press* – (Washington) **Trial begins Monday in firebombing at University of Washington.** A student at Evergreen State College in Washington says she is not sure where she was early on May 21, 2001, but there is one place she was not: crouching in the bushes near a research center at the University of Washington, serving as a lookout for her fellow Earth Liberation Front (ELF) activists as they set firebombs that caused millions of dollars in damage. Prosecutors say that is exactly where she was, and they are intent on proving it during a trial that begins Monday at U.S. District Court in Tacoma. Of more than a dozen environmental and animal-rights activists arrested following a nine-year investigation into ecoterrorism in the Northwest, this student was the only one who has declined to plead guilty. She is taking her chances before a jury because "she's not going to jail or prison for something she did not do," her lawyer said. According to prosecutors, Waters joined four other people in burning down the university's Center for Urban Horticulture that spring night, obtaining a rental car for the group, hiding in the bushes as a lookout, and using a walkie-talkie to warn of a passing police cruiser. The UW fire caused $7 million in damage. Investigators say those fires were among at least 17 perpetrated from 1996 to 2001 by members of an ELF and Animal Liberation Front cell clustered around Eugene, Oregon, and Olympia, Washington, that called itself "the Family."
Source: http://seattlepi.nwsource.com/local/6420ap_wst_ecoterror_trial.html

31. *February 10, Salem News* – (Massachusetts) **Salem court area evacuated in bomb scare; Police say suspicious device was battery 'placed purposefully'.** In Massachusetts, a bomb scare at Salem District Court prompted police to evacuate nearby stores, offices, and a church yesterday morning while the state police bomb squad

investigated an object that turned out to be a battery. Around 10:30 a.m., a court employee spotted a suspicious black box propped against the front door of the courthouse and called police. "As soon as we got down here we recognized this is a potential threat," said a Salem police sergeant, "so we blocked the streets and made sure people were safe." The courthouse is closed on Sundays, but a secretary was there doing work. The first justice of the Salem District Courthouse said it was the second scare at the courthouse in a week. He said someone recently made a threat, so court employees are not taking any chances.
Source:
http://www.salemnews.com/punews/local_story_041235055.html?keyword=topstory

32. *February 10, Daily Iberian* – (Louisiana) **Bomb threat at Franklin High School.** For the second time in as many days, a St. Mary Parish, Louisiana, school was disrupted by a bomb threat Friday. Franklin Senior High School was evacuated Friday morning after a bomb threat was called into 911, according to a news release from the St. Mary Parish School Board. Students were evacuated while police and firefighters searched the school. The threat was the second in two days at St. Mary Parish schools. Centerville High School was the target of a bomb threat on Thursday. According to a St. Mary Parish Sheriff's Office press release, a 14-year-old boy was arrested Friday in connection with the Centerville High School bomb threat.
Source:
http://www.iberianet.com/articles/2008/02/10/news/doc47ae92629726a516085814.txt

[Return to top]

Emergency Services Sector

Nothing to report.

[Return to top]

Information Technology

33. *February 11, Network World* – (National) **Powerful new antiphishing weapon DKIM emerges.** There is a new gun in town, and some of the Internet's most powerful companies – including Yahoo, Google, PayPal, and AOL – are brandishing it in the ongoing battle against e-mail fraud. The new weapon is called DKIM, an emerging e-mail authentication standard developed by the Internet Engineering Task Force. DKIM, which stands for DomainKeys Identified Mail, allows an organization to cryptographically sign outgoing e-mail to verify that it sent the message. DKIM addresses one of the Internet's biggest threats: e-mail fraud. As much as 80 percent of e-mail from leading brands, banks, and Internet service providers is spoofed, according to a report released in late January by the Authentication and Online Trust Alliance (AOTA). AOTA analyzed more than 100 million e-mails from Fortune 500 brands sent over a five-month period. "It's a critical need that IT professionals look at e-mail authentication as a competitive advantage to protect their brands and their customers from these exploits as well as to protect their employees from spoofed or forged e-mail

coming into their networks," says the chairman of AOTA. DKIM proponents say the standard is an important step in rebuilding consumer confidence in e-mail. Under development since 2004, DKIM is finally reaching a critical mass.
Source: http://www.networkworld.com/news/2008/021108-antiphising.html

34. *February 11, IDG News Service* – (National) **Attacks aimed at Adobe Reader, Acrobat flaws intensify.** The flaws disclosed last week in Adobe System's Reader and Acrobat programs have been used to exploit computers since at least January via malicious banner advertisements, security analysts are reporting. Adobe issued patches last Wednesday for Reader and Acrobat, but the company did not detail the flaws. Problems with Adobe's software can potentially affect millions of PC users, since the company's software is widely used to read PDF (Portable Document Format) files. Most people regard PDFs as harmless. "From our standpoint, it appears that this PDF-based attack has been quite successful, affecting many thousands of users throughout the world," read a post on Symantec's Security Response Weblog. The flaws in the programs allow a hacker to create a malicious PDF document. If opened by a victim, that document downloads a malicious Trojan that Symantec calls "Zonebac." Zonebac was first detected in 2006. It shuts off a user's security software as well as downloads other bad software. The latest version also appears to taint search engine results, according to Symnatec. In January, iDefense noticed that the malicious PDF document was being delivered through malicious banner advertisements. Symantec wrote that it is not immediately clear how the PDF file is delivered, but that the banner ads could be redirecting people to other harmful Web sites with the file. Also, spam messages may be carrying the bad file as an attachment. Malicious banner ads can be particularly dangerous since the ads can show up on legitimate Web sites.
Source: http://www.infoworld.com/article/08/02/11/Attacks-aimed-at-Adobe-Reader-Acrobat-flaws-intensify_1.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]

Communications Sector

35. *February 11, New York Times* – (National) **Many obstacles to digital TV reception, study says.** Nearly six million people with digital receivers may still lose TV signals when digital-only broadcasts begin next February, a new study says. The study by Centris, a market research firm in Los Angeles, found gaps in broadcast signals that may leave an estimated 5.9 million TV sets unable to receive as many channels as they did before the changeover. It may affect even those who bought the government-approved converter boxes or a new digital TV. To keep broadcast reception, many viewers may have to buy new outdoor antennas, the study found. The Centris study predicts greater

disruption of service than government agencies like the Federal Communications Commission have acknowledged. The federal government estimates that 21 million American households have primary TV sets that receive only over-the-air signals. But it says most will continue to get a digital signal by means of a digital-to-analog converter box, which costs about $50 to $70. It is helping to underwrite the cost of a converter box by issuing $40 coupons. Centris said it looked at a more detailed method for predicting the coverage pattern of TV signals than the government had used. However, the problems with reception could be far worse, according to engineers who have taken signal measurements. One study of the first HDTV station by the consultant hired to replace the broadcast antennas on the Empire State Building, found that digital signals did not travel as far as either model had predicted. Digital reception is more affected by hills, trees, buildings, and other interference than analog has been. An analog TV picture degrades gradually, getting more snow or ghosting as a signal becomes weaker. But digital TV is subject to the "cliff effect" – the picture is excellent until the signal gets weak and the picture suddenly drops out. The number of sets that the Centris study projects will fail varies from city to city, based largely on the landscape.
Source: http://www.nytimes.com/2008/02/11/technology/11analog.html?ref=technology

36. *February 11, Computer Weekly* – (International) **Data security fears increase among mobile phone users.** Mobile phone users are increasingly worried that PC-based information security risks are threatening their phones, leaving network operators with a choice: protect customers against malware and other threats or lose their business. This emerged from research in the UK, the U.S., and Japan by security software house McAfee. The firm looked into mobile phone users' attitudes to information security threats from mobile networks. The research follows a similar study last year among the operators themselves. A security analyst at McAfee said the risks to mobile phone users compared to those faced by PC users connected to the internet are one to 100. But mobile phone users are increasingly concerned that as applications such as micro-payments and banking move onto their phones, they will attract criminals. The analyst said while their immediate concern was loss of cash, more dangerous was the loss of data, especially personal data that could be used to clone the user's identity or to harass them. He said 58 percent of respondents worried about spam, fraudulent use of subscribed services, and theft of data stored on their phones. He warned of "smishing" attacks, where a criminal tried to induce insecure behavior using an SMS text message.
http://www.computerweekly.com/Articles/2008/02/11/229339/data-security-fears-increase-among-mobile-phone-users.htm

37. *February 10, Associated Press* – (International) **Wireless industry meets in Barcelona.** Wireless industry players place their bets on the future during the four-day Mobile World Congress opening Monday in Barcelona, laying stakes on the next big thing with new product launches, services, and alliances. Is wireless broadband beamed into your home in the future? Will advertisers be invading your mobile phone with location-based advertising? Exactly how personalized will your mobile phone become? And is the time ripe for the Internet's migration into your handset? While more than 50,000 industry officials from major cell phone makers, telecommunications companies, and high-technology firms stake out their next move at the world's largest communications

conference, the winners ultimately will be decided by consumers. One of the big challenges facing the industry is the poor adoption and usage of new services despite millions of dollars spent in marketing. A number of initiatives using mobile technology to improve lives in poor, rural areas will be rolled out.
Source:
http://news.wired.com/dynamic/stories/S/SPAIN_WIRELESS_CONFERENCE?SITE=WIRE&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2008-02-10-15-14-59

[Return to top]

Commercial Facilities Sector

38. *February 9, Chattanooga Times Free Press* – (Tennessee) **Bomb scare closes road.** Police are not sure if a device found under a car at Memorial Hospital in Chattanooga, Tennessee, on Friday afternoon was a bomb, but they did not take any chances. The item, wrapped in a brown paper bag and black duct tape, caused enough alarm to result in a portion of the hospital being evacuated and Glennwood Drive being closed for more than two hours, said a Chattanooga Police spokeswoman. The device may have been part of an ongoing domestic dispute, police said. The package was found under a white Lexus. The car's owner said she has a restraining order against her husband. Police are investigating to determine if the husband had anything to do with the situation and called for assistance from the Bureau of Alcohol, Tobacco, Firearms and Explosives, she said.
Source: http://timesfreepress.com/news/2008/feb/09/bomb-scare-closes-road-part-memorial-hospitala/

[Return to top]

National Monuments & Icons Sector

39. *February 10, Associated Press* – (New Mexico) **Federal agents accuse smuggler of stealing N.M. artifacts.** A ceramic pot and a 1,000-year-old ladle looted from New Mexico's El Malpais National Monument are among the stolen artifacts identified in a five-year federal investigation into the smuggling of Asian and American Indian antiquities. Dozens of federal agents raided a Los Angeles gallery and four museums in Southern California, including the Los Angeles County Museum of Art, searching for artifacts taken from protected archaeological sites in Thailand, Myanmar, China, and New Mexico. "There's no question there is a problem," said the head of the Museum of New Mexico's Office of Archaeological Studies. "There is so much public land, and there are so few enforcement officials in any of the federal agencies. People can get away with looting, at least for the short term."
Source: http://www.lcsun-news.com/ci_8224541

[Return to top]

Dams Sector

40. *February 11, Associated Press* – (Indiana) **Flood victims focus ire on utility's dams.** In Indiana, two severe floods within a month downstream from a pair of NIPSCO-owned dams have some homeowners saying the utility company failed to protect them. The company, however, says heavy rains and melting snow caused record water flows on the Tippecanoe River and that its dams were not meant for flood control. A NIPSCO spokesman said the hydroelectric dams, which form lakes Freeman and Shafer about 20 miles north of Lafayette, are "run of the river" dams. "Whatever water flow comes into the dam, we discharge from the dam," he said. "We don't have a reservoir for control, nor are we licensed for flood control."
Source:
http://www.indystar.com/apps/pbcs.dll/article?AID=/20080211/LOCAL/802110393

41. *February 10, Washington Post* – (District of Columbia) **Flood levee ideas rattle panel.** The U.S. Army Corps of Engineers has unveiled three proposals for a flood levee on the Mall that would require permanent foundations on both sides of 17th Street and a system of temporary vertical girders and metal panels that would be erected during a flood. All three proposals call for what is known as a post-and-panel levee, which would be designed to block Potomac River floodwater flowing north on 17th Street, experts said. Such a levee would be erected just above the World War II Memorial at a cost of about $8 million, officials said. The proposals were detailed Thursday during a meeting of the National Capital Planning Commission, where the Corps and the Federal Emergency Management Agency explained the rationale for FEMA's proposed new flood maps, which place much of downtown Washington in a flood-hazard zone.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/02/09/AR2008020902295.html

42. *February 9, Republican* – (Massachusetts) **State orders breach to avert dam failure.** Massachusetts issued an emergency order yesterday to breach an Indian Orchard dam in order to prevent it from failing and releasing 30 million gallons of water downstream toward a mobile home park. Crews with heavy construction equipment began tearing a hole in the large earthen dam at Bircham Bend Pond yesterday afternoon. The property is owned by Solutia and the Postal Service, said the city's director of emergency preparedness. A beaver dam blocked a culvert downstream, causing rainwater to flood a ravine between the culvert and the earthen dam. Officials said they feared the culvert could open suddenly, causing the pooled water to drain quickly. This could weaken the earthen dam and cause it to fail.
Source: http://www.masslive.com/chicopeeholyoke/republican/index.ssf?/base/news-12/1202545253105240.xml&coll=1

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Distribution Information:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

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

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.