Department of Homeland Security Daily Open Source Infrastructure Report for 1 February 2008

Current Nationwide

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here

- According to the Associated Press, the new rules for the types of identification U.S. or Canadian citizens must present to cross into the country should not cause significant delays and will not be strictly enforced at first. These rules come into effect on January 31. (See item **15**)
- The Associated Press obtained hundreds of pages of heavily censored files detailing the February 2006 "Cyber Storm" war game conducted by the DHS with the help of numerous other government departments and agencies. The exercise was run to test the nation's hacker defenses, simulating what were described as plausible, detailed attacks against the technology industry, transportation lines, and energy utilities by anti-globalization hackers. A second run, "Cyber Storm 2," is planned for March. (See item **27**)

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. *January 31, Associated Press* – (National) **Fierce winds rip across nation.** Lake Erie surged over its eastern shore yesterday, adding flooding to the headaches delivered by a windy storm. It tipped tractor-trailers, disrupted flights, and toppled trees and power lines across a wide swath of the nation. The severe weather was part of a storm system that knocked out power to thousands in upstate New York, West Virginia, Ohio, and

Illinois. In Michigan, Lower Peninsula residents were in the dark as blizzard conditions hit the western and northern parts of the state.
Source: http://www.inrich.com/cva/ric/news.apx.-content-articles-RTD-2008-01-31-0170.html

2. *January 31, Midland Reporter-Telegram* – (National) **DOE restructures FutureGen concept to encourage more rapid commercialization.** A day after announcing it was pulling out of the FutureGen project over concerns about the ballooning costs of the next-generation power plant utilizing clean coal technology, the Department of Energy (DOE) unveiled its new vision for the project. The energy secretary announced Wednesday that, rather than focusing on and funding one site that would be what he called a living laboratory, the agency instead would encourage industry to build multiple sites utilizing clean coal technology – whether it is Integrated Gasification Combined Cycle or post-combustion technology – with an added carbon capture and storage (CCS) component. "This would allow for clean coal-powered plants to add CCS as soon as they're commissioned, which should be about 2015," he said in a telephone news conference. "This will allow multiple locations to develop clean coal technology and at least double the amount of carbon dioxide sequestered compared to the original concept." With the announcement of this new approach, the agency has issued a Request for Information seeking industry input on the cost and feasibility of building clean coal plants that achieve FutureGen's goals. The comment period will end March 3. The deputy secretary of energy said input received from the utilities industry will determine how many sites can be commissioned.
Source: http://www.mywesttexas.com/site/news.cfm?newsid=19249419&BRD=2288&PAG=461&dept_id=475626&rfi=6

[Return to top]

Chemical Industry Sector

3. *January 31, Politico* – (National) **Security, commerce suffer chemical imbalance.** Legislation designed to protect the nation's chemical plants from terrorist attack has sparked a lobbying ruckus in the House among the industry, environmentalists, and labor unions. At the center of the debate: the 4,400 facilities across the nation considered potential targets because they contain dangerous chemicals. Pressure on Congress to enact a chemical plant security regime is increasing because the Department of Homeland Security is operating under a temporary law that will sunset next year. In January, the department began processing reports from more than 16,000 facilities across the country to determine their vulnerability to attack. DHS estimated that about 100 of the riskiest plants might be forced to change their practices, unless a facility can justify its current practices on economic or technological grounds. Facilities considered less risky are required to submit an assessment outlining options for such changes but are not required to act on it. This concept, known as inherently safer technology, or IST, is the cause of major consternation to the chemical industry, which objects to the government's interfering in its business. Manufacturers are worried about losing sales if plants using the chemicals switched to safer alternatives, he said. Water treatment plants

are particularly vulnerable because of their use of chlorine gas, he noted, but some have switched to safer alternatives such as liquid bleach and ultraviolet light.
Source: http://www.politico.com/news/stories/0108/8220.html

4. *January 30, Associated Press* – (Minnesota) **Study finds 3M chemicals found in more Twin Cities lakes.** A chemical formerly manufactured by 3M Co. has been found at elevated levels in nine more lakes in the Twin Cities region, Minnesota, likely entering the lakes through stormwater runoff, according to a study. The Minnesota Pollution Control Agency collected fish from 20 lakes and two river reaches last spring and summer and analyzed the fish for PFOS (perfluorooctane sulfonate) and related compounds. The company made the chemical for decades for Scotchgard, firefighting foams, and other products before ceasing production in 2002. The lakes study, released Tuesday, began after the discovery last spring of relatively high levels of PFOS in bluegills from Lake Calhoun in Minneapolis. That prompted authorities to advise anglers to eat no more than one meal per month of bluegills taken from Calhoun and four connecting lakes. State health officials said in a prepared statement that they would evaluate the findings and determine whether additional warnings about fish consumption will be issued.
Source:
http://www.thedickinsonpress.com/ap/index.cfm?page=view&id=D8UGCCMO0

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *January 31, Miami Herald* – (Florida) **FPL asks panel to allow two more nuclear reactors.** Florida Power & Light (FPL) began making its case to state regulators on Wednesday that the two nuclear reactors it wants to add at Turkey Point are the best option for keeping South Florida humming. "Nuclear power is the backbone for FPL's system, providing safe and low-cost energy, 24-7," an FPL attorney told the Public Service Commission (PSC), which opened a three-day hearing in Tallahassee on what could be Florida's first expansion of nuclear power in decades. Environmentalists and a state-assigned consumer advocate questioned FPL's claims, arguing the utility has not calculated some big-ticket costs, starting with the bill for up to 80 million gallons a day of cooling water. FPL's plans face years of state and federal reviews on environmental, safety, and design issues. The PSC hearing is a critical hurdle that could clear the way for major expansion of the complex near Homestead. A decision from the five commissioners – appointed by the governor to oversee power, phone, gas, and water utilities – could come as soon as mid-March.
Source: http://www.miamiherald.com/news/miami_dade/story/400489.html

6. *January 30, PPL Corporation* – (Pennsylvania) **PPL's Susquehanna plant approved to increase generating capacity.** The U.S. Nuclear Regulatory Commission (NRC) on Wednesday gave permission for an increase in the amount of electricity PPL's Susquehanna nuclear plant in Luzerne County, Pennsylvania, can safely generate. "This plant has a proven record of safely and reliably producing electricity," said PPL's senior vice president and chief nuclear officer. "Increasing its capacity is a cost-effective way

to meet the increasing demand for electricity in the region from an existing resource." The two reactors at the Susquehanna plant were designed and built to operate at the increased power level. PPL's application to the NRC included an extensive safety report and environmental assessment that received a detailed review by the commission. The increase will total about 205 megawatts, which is enough electricity to supply about 160,000 homes. The increase will be implemented in phases between 2008 and 2010 as plant modifications are completed.
Source: http://money.cnn.com/news/newsfeeds/articles/prnewswire/NEW11830012008-1.htm

7. *January 30, Post-Standard* – (Maryland; New York) **New York not Maryland may get first new nuke plant.** Constellation Energy – the owner of two nuclear plants in Scriba, New York – said it may build its first new nuclear plant in New York if Maryland regulators prove too hostile. A number of companies are planning to propose new plants in the coming years, according to the U.S. Nuclear Regulatory Commission. Constellation is scheduled to apply for a license to operate a plant in Maryland. The company had said it would like to break ground at Calvert Cliffs, Maryland, this year. "However, if we encounter delays in Maryland, we are prepared to proceed with the first EPR [new nuclear reactor] at our Nine Mile Point nuclear plant location in New York," said Constellation's executive vice president in a press release Tuesday. Constellation has begun environmental studies at both the Calvert Cliff and Nine Mile Point sites. The Maryland site – not far from the headquarters of Constellation and UniStar Nuclear Energy, the joint venture created to build a new plant – is further along than any of a number of potential sites for future nuclear plants. Energy demand in Maryland is outstripping supply, and, without a new plant or new transmission lines to bring power from elsewhere, officials have said Maryland could run out of power.
Source: http://blog.syracuse.com/news/2008/01/report_scriba_not_maryland_may.html

[Return to top]

Defense Industrial Base Sector

8. *January 31, Associated Press* – (National) **Boeing, Bell team wins $32M Navy deal.** A strategic alliance of Boeing Co. and Textron Inc.'s Bell Helicopter operation has won a Navy contract worth up to $32 million to handle weather radar upgrades on the V-22 Osprey, a tiltrotor vertical/short takeoff and landing aircraft.
Source: http://www.businessweek.com/ap/financialnews/D8UGR4Q80.htm

9. *January 31, Associated Press* – (National) **Boeing wins $24.1M Navy contract.** Boeing Co. has been awarded a $24.1 million contract to supply parts for the Navy's F/A-18 Hornet fighter and attack aircraft, the Defense Department said late Wednesday. The contract is a follow-on to an existing award to support the F/A-18, which is built by Boeing's McDonnell Douglas unit.
Source: http://www.businessweek.com/ap/financialnews/D8UGR3SO0.htm

10. *January 30, Lockheed Martin* – (National) **Lockheed Martin receives $512 million contract for HIMARS and GMLRS.** Lockheed Martin has received a $512 million

contract to provide the High Mobility Artillery Rocket System (HIMARS) and the Guided Multiple Launch Rocket System (GMLRS) to the U.S. Army and to the U.S. Marine Corps. Work on the contract will be performed at the company's facilities in Camden, Arkansas, and Grand Prairie, Texas, and is scheduled for completion in fourth quarter 2010. Specific quantities of vehicles and rockets were not disclosed.
Source: http://money.cnn.com/news/newsfeeds/articles/prnewswire/LAW08730012008-1.htm

[Return to top]

Banking and Finance Sector

11. *January 31, Associated Press* – (National) **IRS warns of rebate scams.** Even before Congress passes an economic stimulus package, identity thieves are using promises of tax rebates to trick people into revealing financial and personal data, the Internal Revenue Service warned Wednesday. In one scheme, the IRS said, people are receiving phone calls telling them they can only receive a rebate if they provide bank account information for a direct deposit. In another, a caller claims to be an IRS employee who says the taxpayer has not cashed a refund check and asks the person to verify his or her bank account number. The tax agency stressed that it does not collect information by telephone and that no legislation has been enacted that would allow it to provide advance payments to taxpayers or that specifies the details of those payments. Another scam, it said, involves an e-mail notification that a person's tax-return will be audited with instructions to click on links to complete forms with personal and account information. Businesses and accountants are also getting e-mails with instructions to download information on tax law changes. Clicking on these links could download "malware" onto the recipient's computer that gives the scammer remote access to the computer hard drive. The IRS advised people not to click on any link from an e-mail purporting to come from the tax agency. People receiving questionable e-mails can contact the IRS through phishing@irs.gov.
Source: http://money.cnn.com/2008/01/31/pf/taxes/bc.irs.scams.ap/index.htm?cnn=yes

12. *January 31, ComputerWeekly* – (National) **Two-factor banking security systems threatened by Trojan.** The new Trojan, spotted in various forms in recent weeks, poses a potentially serious threat to most authentication systems being rolled out by banks to protect their electronic customers. "Most of the banks' two-factor authentication systems center around the use of a customer-supplied password, plus a unique, one-time code generated by an electronic token such as a SecurID unit or a user's mobile phone," said the CTO at security behavioral analysis firm Tier-3. "This new Trojan, called Silentbanker, allows hackers intermediary access to the information stream from the user, allowing them to create a man in the middle type attack during an e-banking session. This effectively counters the protection afforded to users by the two-factor authentication technology," he said. The official said updated security software should spot the Trojan, but he added that modified versions of the threat could potentially evade established security systems.
Source: http://www.computerweekly.com/Articles/2008/01/31/229191/two-factor-banking-security-systems-threatened-by-trojan.htm

13. *January 30, InformationWeek* – (National) **Davidson Companies reports data breach affecting 226,000 clients.** Davidson Companies said on Wednesday that a database containing personal information of 226,000 current and past clients, including names and social security numbers, appears to have been illegally accessed "by a third party through a sophisticated network intrusion." The company reportedly hired a penetration testing company last September to assess its IT security and the firm's hackers did not find any holes. A company spokesperson declined to provide further details. The company said in a statement that it has found no evidence that those who hacked its systems have been able to affect or alter client data. Nonetheless, the company is urging clients to be on guard against identity theft fraud that could arise as a result of the data breach. To assist those affected, the company plans to pay for a year of credit monitoring service.
Source:
http://www.informationweek.com/news/showArticle.jhtml?articleID=206100536

14. *January 30, InformationWeek* – (New Jersey) **Laptop stolen with personal data on 300,000 health insurance clients.** Horizon Blue Cross Blue Shield of New Jersey has notified its members that an employee laptop computer containing personal information -- including Social Security numbers -- for about 300,000 individuals was stolen in Newark, New Jersey, on January 5. On its Web site, the company says a "security feature was initiated" on January 28 that "destroys all the data on the stolen computer." Horizon Blue Cross Blue Shield of New Jersey says the personal information contained on the computer also included names and addresses of members, but no medical data. The company says it "believes" it is "highly unlikely" that any personal data stored on the stolen computer has been accessed and that the computer was "password protected." Nonetheless, the insurer is offering affected members free credit monitoring for one year.
Source:
http://www.informationweek.com/news/showArticle.jhtml?articleID=206100526

[Return to top]

Transportation Sector

15. *January 31, Associated Press* – (National) **Homeland Security requires border crossers to show extra ID.** New rules for the types of identification U.S. or Canadian citizens must present to cross into the country should not cause significant delays and will not be strictly enforced at first, a senior federal official said. Under the rules going into effect Thursday, people will no longer be allowed to simply declare to immigration officers at border crossings that they are citizens, a deputy commissioner with U.S. Customs and Border Protection said Tuesday. Instead, those 19 and older will have to show proof of citizenship – a passport, trusted traveler card, or a birth certificate and government-issued ID such as a driver's license. Drivers' licenses enhanced with proof of citizenship and a radio frequency identification chip also will be accepted, he added. He also said officers at the ports will have latitude to admit people who are unaware of the changes once their identities are confirmed. Over the last two fiscal years, 31,000

people who claimed at the borders to be U.S. citizens were not, he said. A spokesman for U.S. Customs and Border Protection in Detroit, which has the busiest northern border crossing, also said the agency will provide a grace period for travelers without the extra ID, and will hand out fliers explaining the changes. Congress approved the Western Hemisphere Travel Initiative in 2004, which requires verified citizenship and identification of all those entering the country from Canada, Mexico, and the Caribbean. The passport requirement for land and sea crossings has been delayed until June 2009.
Source: http://www.foxnews.com/story/0,2933,326990,00.html

16. *January 31, Associated Press* – (Florida) **U.S. flight makes emergency landing after cockpit fills with smoke.** Smoke filled the cockpit of an American Airlines flight from Puerto Rico, forcing an emergency landing, a Palm Beach International Airport official said. Seven people — the pilot, co-pilot, three flight attendants and two passengers — were taken to a hospital Wednesday, but none of the injuries was life threatening. A windshield was also broken, but the reason was unclear. The plane had left San Juan for Philadelphia and landed safely at Palm Beach International Airport, said an airport spokeswoman. The Federal Aviation Administration is investigating.
Source: http://www.foxnews.com/story/0,2933,326949,00.html

17. *January 30, Aviation* – (National) **U.S. air traffic controller force in crisis.** Higher-than-forecasted air traffic controller retirements and total controller attrition over the past few years have left the United States with the lowest number of fully trained and certified controllers since 1992, according to the National Air Traffic Controllers Association. By the end of 2007 there were 11,250 fully qualified controllers working at the Federal Aviation Administration's 314 facilities. According to NATCA, since 2004 the FAA has significantly underestimated the number of controllers who will retire, and this has contributed to the current controller shortage. Earlier this month, the NATCA president said that remaining veteran controllers no longer can handle peak volumes in Atlanta, Chicago, New York, and Southern California safely. He indicated that a controller staffing emergency exists in the four locations, which are among the most congested in the country. The FAA's chief operating officer acknowledged that staffing is "tight" at "a few facilities." But he emphasized that "nothing in our data shows any increase of errors where staffing or fatigue have been contributory. We do not believe we are running an unsafe system." NATCA said in an October 22, 2007 news release that, while there were 3,618 controller trainees system-wide, approximately one-third of them were not certified on any position and could not work alone without a fully certified controller beside them. However, the FAA official said the agency is aggressively hiring new controllers and is pleased with their skills and progress in training. New controllers can take up to three years to become fully certified for all tasks at busy facilities.
Source: http://www.msnbc.msn.com/id/22917202/

[Return to top]

Postal and Shipping Sector

18. *January 30, Orange County Register* – (California) **Powder scare shuts Scientology centers in Tustin, Newport.** A series of letters containing a white, powdery substance were received Wednesday by at least nine Church of Scientology-affiliated buildings across Southern California, authorities said. Initial tests done by fire and police agencies found the substances to be harmless. The powder sent in the two of the envelopes was cornstarch and wheat germ, said a lieutenant with the Tustin Police Department. At least one of the envelopes contained threats, demanding the Church of Scientology be dismantled. The FBI is investigating the synchronized threats, which were delivered by the U.S. Postal Service. No arrests have been made.
Source: http://www.ocregister.com/news/powder-church-strain-1970259-scientology-cornstarch

[Return to top]

Agriculture and Food Sector

19. *January 31, CNN* – (California) **Video of workers abusing cows raises food safety questions.** A video showing Hallmark Meat Packing Co. slaughterhouse workers abusing dairy cows was released by the Humane Society of the United States on Wednesday. The video, which one lawmaker said raises questions about the safety of the nation's food supply, shows workers administering repeated electric shocks to "downed cows" that are too sick, weak, or otherwise unable to stand on their own. Workers are seen kicking cows, jabbing them near their eyes, ramming them with a forklift and shooting high-intensity water up their noses in an effort to force them to their feet for slaughter. The society says the video was shot last year by an undercover investigator who wore a hidden camera under his clothes when he worked at the facility. Hallmark Meat Packing Co., based in Chino, California, sells beef to its sister company, Westland Meat, which distributes it to various federal programs, including the National School Lunch Program. Downed cows are more easily contaminated and may carry diseases harmful to consumers. U.S. Department of Agriculture regulations prohibit allowing disabled or contaminated animals into the food supply. Officials said they would investigate.
Source: http://www.cnn.com/2008/US/01/30/undercover.slaughter.video/index.html

20. *January 30, New York Times* – (National; New York) **More testing of seafood to address mercury concerns.** A number of restaurants and retailers in different parts of the country have started testing the fish they sell in response to concerns about the amount of mercury in seafood, and the Environmental Protection Agency is beginning to examine the mercury content in fish sold in the New York City region. The regional office of the federal agency, which began the study because the city found high levels of mercury in the blood of New Yorkers last spring, will examine the 20 most commonly eaten fish in the region, including tuna. Recent laboratory tests reported last week in the New York Times found so much mercury in some sushi made with tuna, particularly bluefin, that a long-term diet of even two or three pieces a week would exceed the levels considered acceptable by the Environmental Protection Agency. The National Fisheries Institute said that the mercury levels found in seafood eaten in the U.S. did not present a health risk. But many scientists suggest that it is best for people to choose fish with low

mercury levels and high levels of beneficial fatty acids.
Source: http://www.nytimes.com/2008/01/30/dining/30mercury.html?_r=1

21. *January 30, Reuters* – (Illinois) **USDA declares 61 counties in Illinois disaster area.** The U.S. Agriculture Department on Wednesday declared 61 counties in Illinois as primary disaster areas, a move that will make farmers eligible for low-interest emergency loans. USDA said the counties had losses caused by drought between April 1, 2007, and December 31, 2007.Additional counties in Illinois, Indiana, Kentucky, and Missouri are eligible for assistance because they are close to the primary disaster areas.
Source: http://www.reuters.com/article/bondsNews/idUSN3023678020080130

[Return to top]

Water Sector

22. *January 31, Washington Post* – (District of Columbia) **Residents seek reassurance on safety of drinking water.** The District of Columbia Water and Sewer Authority officials faced heated questions and concerns last night from a small group of residents and activists at a meeting about the utility's idea to scale back its replacement of lead water pipes across the city. The general manager told residents that District drinking water meets federal guidelines since a chemical was added in 2004 to prevent lead leeching from pipes and that no significant health issues have been detected. The authority also replaced nearly half of its 35,000 lead pipes in public space at a cost of $93 million, he said. Officials faced strong criticism from the crowd when they explained that the partial replacement program, which replaces pipes on public property while relying on homeowners to replace lines on private property, had not resulted in a significant change in lead levels, but could not provide detailed data.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/01/30/AR2008013004275.html

23. *January 30, Sacramento Business Journal* – (California) **Dixon fined $220,000 for water pollution.** A state water quality regulator fined the city of Dixon, California, $220,000 for allegedly polluting groundwater in Solano County. The Central Valley Regional Water Quality Control Board had issued the city three cease-and-desist orders for the city's wastewater treatment plant in 1996, 1997, and 2005 because of insufficient capacity and groundwater pollution, according to a water board press release. The board said the city has never fully complied with those orders and has taken no action to alleviate the problem, caused by excessive salt in the city's sewage. The city has asked for more time to comply with the order.
Source: http://www.bizjournals.com/eastbay/stories/2008/01/28/daily53.html

[Return to top]

Public Health and Healthcare Sector

24. *January 31, Winston-Salem Journal* – (National) **Studies find mutated flu bug that is resistant to antiviral.** A small percentage of the main influenza virus causing illness

this winter in the United States, Europe, and Canada has a mutation that makes it resistant to the antiviral drug Tamiflu, the World Health Organization said yesterday. Scientists said they were surprised because they had believed that mutations of this type generally made the virus less easily spread. There are no immediate plans to recommend changes in the use of Tamiflu, officials said.
Source:
http://www.journalnow.com/servlet/Satellite?pagename=WSJ%2FMGArticle%2FWSJ_BasicArticle&c=MGArticle&cid=1173354428578&path=!nationworld&s=1037645509161

25. *January 30, Associated Press* – (International) **Bird flu sweeps Indonesia, India, Tibet.** Bird flu killed its third victim in as many days in Indonesia, raising the country's human toll to 101, and ravaged poultry stocks in Tibet and India on Wednesday, as the virus spreads across Asia. In southwestern Tibet, a poultry farm was quarantined after an outbreak killed 1,000 birds, agriculture officials reported Wednesday. More than 13,000 other poultry were killed to prevent its spread. In India, the virus spread in three districts of West Bengal state, where culling was under way and more than 129,000 poultry birds have died, said the Animal Resource Development Minister. Health workers have killed nearly 2.5 million at-risk birds and were clearing areas within three miles of infection sites, the minister said. No human infections have been recorded. Officials in neighboring Bangladesh ordered the halt of all egg and poultry imports from India.
Source:
http://ap.google.com/article/ALeqM5hutx99h4P3zhm9sOE7F_ZO3qVGIwD8UG96N80

Government Facilities Sector

Nothing to report.

[Return to top]

Emergency Services Sector

26. *January 31, Associated Press* – (National) **US military not adequately prepared for homeland attack, report says.** The U.S. military is not ready for a catastrophic attack on the country, and National Guard forces do not have the equipment or training they need for the job, according to a report. Even fewer Army National Guard units are combat-ready today than were nearly a year ago when the Commission on the National Guard and Reserves determined that 88 percent of the units were not prepared for the fight, the panel says in a new report released Thursday. The independent commission is charged by Congress to recommend changes in law and policy concerning the Guard and Reserves. The commission's 400-page report concludes that the nation "does not have sufficient trained, ready forces available" to respond to a chemical, biological, or nuclear weapons incident, "an appalling gap that places the nation and its citizens at greater risk." "Right now we don't have the forces we need, we don't have them trained, we don't have the equipment," said the commission chairman in an interview with the

Associated Press. In response, the Air Force general in charge of U.S. Northern command said the Pentagon is putting together a specialized military team that would be designed to respond to such catastrophic events. The capability for the Defense Department to respond to a chemical, biological event exists now," he told the AP. "It, today, is not as robust as we would like because of the demand on the forces that we've placed across the country. ... I can do it today. It would be harder on the (military) services, but I could respond." Over the next year, he said, specific active duty, Guard and Reserve units will be trained, equipped, and assigned to a three-tiered response force totaling about 4,000 troops. There would be a few hundred first responders, who would be followed by a second wave of about 1,200 troops that would include medical and logistics forces. The third wave, with the remainder of those initial 4,000 troops, would include aircraft units, engineers, and other support forces, depending on the type of incident.
Source:
http://seattletimes.nwsource.com/html/nationworld/2004156194_webmilitary31.html

[Return to top]

Information Technology

27. *January 31, Associated Press* – (National) **Trains, bloggers are threats in US drill.** It is the government's idea of a really bad day: Washington's Metro trains shut down. Seaport computers in New York go dark. Bloggers reveal locations of railcars with hazardous materials. Airport control towers are disrupted in Philadelphia and Chicago. Overseas, a mysterious liquid is found on London's subway. Those incidents were among dozens of detailed, mock disasters confronting officials rapid-fire in the U.S. government's biggest-ever "Cyber Storm" war game, according to hundreds of pages of heavily censored files obtained by the Associated Press. The Homeland Security Department ran the exercise to test the nation's hacker defenses, with help from the State Department, Pentagon, Justice Department, CIA, National Security Agency, and others. The laundry list of fictional catastrophes – which include hundreds of people on "No Fly" lists suddenly arriving at airport ticket counters – is significant because it suggests what kind of real-world trouble keeps people in the White House awake at night. Imagined villains include hackers, bloggers, and even reporters. After mock electronic attacks overwhelmed computers at the Port Authority of New York and New Jersey, an unspecified "major news network" airing reports about the attackers refused to reveal its sources to the government. Other simulated reporters were duped into spreading "believable but misleading" information that worsened fallout by confusing the public and financial markets, according to the government's files. The $3 million, invitation-only war game simulated what the U.S. described as plausible attacks over five days in February 2006 against the technology industry, transportation lines, and energy utilities by anti-globalization hackers. The incidents were divided among categories: computer attacks, physical attacks, or psychological operations. The exercise had no impact on the real Internet. Officials said they were careful to simulate attacks only using isolated computers, working from basement offices at the Secret Service's headquarters in downtown Washington. However, the government's files hint at a tantalizing mystery: In the middle of the war game, someone quietly attacked the very

computers used to conduct the exercise. Perplexed organizers traced the incident to overzealous players and sent everyone an urgent e-mail marked "IMPORTANT!" reminding them not to probe or attack the game computers. The government is organizing another multimillion-dollar war game, Cyber Storm 2, to take place in early March.
Source: http://news.yahoo.com/s/ap/20080131/ap_on_go_ca_st_pe/cyber_storm;_ylt=AjIUA7JpdaOB_a7rOwdWpLqDzdAF

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

28. *January 31, Associated Press* – (International) **Indian outsourcing firms hit hard by Internet outage.** India's lucrative outsourcing industry struggled Thursday to overcome Internet slowdowns and outages after cuts in two undersea cables sliced the country's bandwidth in half. The disruption – which has hit a swath of users from Egypt to Bangladesh – began to affect much of the Middle East on Wednesday, when outages caused a slowdown in traffic on Dubai's stock exchange. The cables, which lie off the coast of Egypt in the Mediterranean, were snapped as the working day was ending in India on Wednesday and the impact was not immediately apparent. But by Thursday, the Internet was sluggish across the country with some users unable to connect at all and others frustrated by spotty service. The Internet Service Providers' Association of India said the country had lost half its bandwidth. In all, users in India, Pakistan, Egypt, Qatar, Saudi Arabia, the United Arab Emirates, Kuwait, and Bahrain were affected. Engineers in several countries were scrambling to reroute traffic to satellites and to other cables. The biggest impact to the rest of the world could come from the outages across India, where many U.S. companies outsource customer-service call centers and other back-office operations. Officials said it could take a week or more to fix the cables, apparently cut north of the Egyptian port city of Alexandria. A top Egyptian telecommunications official said that workers would not know for sure what caused the cuts until they are able to get repair ships and divers to the area, though there was speculation a ship's anchor was to blame. Rough weather and seas prevented repair ships from getting to the site Wednesday, the official said and it was unclear how soon they could get there. Even once the repair workers arrive at the site, it could take as long as a week to repair the cable, the official said. India has built up massive amounts of bandwidth in recent years and is likely to be able to handle the situation without major economic losses, analysts said.
Source: http://www.foxnews.com/story/0,2933,326988,00.html

29. *January 30, Ars Technica* – (International) **US tops world Connectivity Scorecard despite broadband ills.** When it comes to using information technology well, people power is as important as wires, chips, and radio signals. That is one of the assumptions driving the new Connectivity Scorecard benchmark put together by a researcher from the London Business School. The study found that the U.S. takes the worldwide lead on "connectivity" when measured in this way, but sub-par broadband infrastructure holds the country back. The study was sponsored by Nokia Siemens, and it attempts to measure how "usefully connected" countries are, not just how much raw infrastructure they possess. As the author put it, only "smart" usage "helps make Connectivity a driver of productivity gains and hence economic growth." Because of this focus, the scorecard rankings look a bit different than other, similar charts. Korea comes in tenth, for instance, even though it is a top performer on most technology metrics. According to the research, though, "very high performance in infrastructure is not matched by correspondingly high scores on usage measures, especially by businesses." Despite being docked for broadband, the U.S. skill set and deep level of IT use among businesses put the country on top. Sweden and Japan take the next two spots. The highest possible score was ten, and the fact that no country scored higher than a seven shows that there is plenty of room for growth. No country did well on all metrics, either. Even the U.S., which led the field, did not rank first in any of the main areas (business, consumer, and government), and the report points out that certain functions like mobile banking are actually "better developed in African countries than in the U.S. or Canada." Among developing economies, Russia and Malaysia took the top two spots for their high literacy rates and wide usage of IT.
Source: http://arstechnica.com/news.ars/post/20080130-us-tops-world-connectivity-scorecard-despite-broadband-ills.html

[Return to top]

Commercial Facilities Sector

30. *January 31, AT&T* – (Tennessee) **AT&T survey finds that disaster preparedness not a priority for nearly one-fourth of Tennessee businesses in Nashville and Memphis.** Although threats of devastating natural disasters, terrorist attacks, and other man-made calamities have prompted more U.S. businesses to prepare for disaster, AT&T Inc. announced that a survey of local executives indicates many businesses in Memphis and Nashville still remain vulnerable. The survey of 100 local information technology executives found that Memphis and Nashville scored better than half of the U.S. cities surveyed for disaster preparedness, including Atlanta, Chicago, and Los Angeles, but nearly one-fourth (23 percent) of respondents still say business continuity is not a priority. Businesses in the Memphis and Nashville area ranked fifth among 10 U.S. metropolitan areas surveyed by AT&T. Planning ahead for man-made calamities is also important. The survey found that approximately eight out of ten (85 percent) of the Memphis and Nashville respondents said that cybersecurity is part of their overall business continuity plan. When asked what keeps them up at night, Memphis and Nashville respondents most frequently said computer viruses and worms (32 percent), followed by security breaches (23 percent), and natural disasters (23 percent). For more information on the AT&T 2007 Business Continuity study, including the complete

report, visit http://www.att.com/biz_continuity_study_2007.
Source:
http://money.cnn.com/news/newsfeeds/articles/prnewswire/AQTH02931012008-1.htm

[Return to top]

National Monuments & Icons Sector

31. *January 31, Jackson Hole Daily* – (Wyoming) **Company proposes drilling in Wyoming Range.** Just days after Bridger-Teton National Forest officials announced the start of a new environmental analysis for 44,700 acres in the Wyoming Range, an energy company has proposed a plan to drill on part of the contested land. Officials with Stanley Energy of Denver have proposed 181 wells on roughly 29,000 acres. The company would exchange current leases for permission to drill on more than 20,000 of the 44,700 contested acres. The proposal would involve eight 50-acre well pads for a total surface disturbance of 400 acres. The Forest Service announced plans for a supplemental environmental impact statement on the 44,700 acres Monday, after the federal Interior Board of Land Appeals ruled that an earlier National Environmental Policy Act analysis failed to sufficiently analyze impacts to wildlife and the environment. The 44,700 acres also are included in proposed legislation that would allow the buyout of Wyoming Range leases. The bill would protect more than 1.2 million acres of the range from future leasing and would allow existing leases to be bought back and the land preserved. It is currently in the U.S. Senate Committee on Energy and Natural Resources.
Source: http://www.jhguide.com/article.php?art_id=2689

[Return to top]

Dams 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 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.