Department of Homeland Security Daily Open Source Infrastructure Report for 23 January 2006

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

Daily Highlights

- The Transportation Security Administration has announced several parameters for a nationwide private sector Registered Traveler program, including the biometrics to be used for identification purposes and the redress process for individuals who are denied access to the program. (See item 10)
- The Times Herald reports a network of chemical monitors could soon be protecting Michigan's drinking−water plants, providing nearly instantaneous detection of chemical spills to the St. Clair River and Lake St. Clair. (See item 25)

DHS Daily Open Source Infrastructure Report *Fast Jump*

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

Energy Sector

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

1. *January 21, Associated Press* — **No gasoline in Illinois during disasters?** Many of Illinois' independent gasoline stations may consider temporarily shutting down if a disaster similar to Hurricane Katrina hits, insulating themselves from future claims of gas gouging. Bill Fleischli, executive vice president of the Illinois Petroleum Marketers Association, whose group's 500 members supply or own all but roughly 1,000 of the state's 4,500 gas stations statewide, said "For an owner to be concerned about the ramifications of raising prices is not right, and I don't think that's the way the American system should work," he said. Attorney General Lisa

Madigan had accused 18 gas stations of unjustifiably high prices after Hurricane Katrina slammed the Gulf Coast in August. Last week, her office said those stations each have agreed to donate $1,000 each to the Red Cross to avoid being sued by the state, although the gas stations insist they did nothing wrong. Those businesses, Fleischli said, merely passed along higher costs, with the $3−a−gallon sale price in some areas reflecting the value of dwindling gasoline reserves.
Source: http://www.suburbanchicagonews.com/couriernews/top/3_1_EL21_A1GAS_S1.htm

2. *January 21, Associated Press* — **Gas leak prompts high−tech detection tools.** The United States has 2.3 million miles of natural gas pipeline. Errant bulldozers, imperfect seals, and other mishaps, disasters, and defects cause leaks. According to industry and government estimates, 1.5 percent is leaked into the air. That percentage is significant because the U.S. burns so much gas that the leakage could fuel about four million more homes, government statistics indicate. Government standards mandate leak surveys up to four times a year along pipelines. Almost $20 billion is needed just to replace existing pipe by the end of the next decade, according to one industry study. New types of scanners typically beam invisible infrared light — at wavelengths absorbed only by methane or some other component of natural gas. Handheld remote detectors reached the market last spring. Other emerging technologies include camera−like detectors that analyze ordinary reflected daylight from a helicopter at 1,000 feet, finding leaks from space with satellites, and very small robots to home in on trouble spots. Future pipelines might even carry built−in sensors to alert to rusting, cracking, or outright leaks.
Source: http://news.yahoo.com/s/ap/20060121/ap_on_hi_te/into_thin_air_1

3. *January 20, Associated Press* — **Nuclear plant owner fined $28 million for covering up serious damage.** Acknowledging that its employees covered up serious damage at the Davis−Besse nuclear power plant, the facility's owner, FirstEnergy Corp., has agreed to pay $28 million in fines, restitution and community service projects, the U.S. Justice Department announced Friday, January 20. Inspectors found an acid leak in 2002 that nearly ate through a six−inch (15−centimeter) steel cap on the reactor vessel. Officials said it was the most extensive corrosion ever seen at a U.S. nuclear reactor. Company and Nuclear Regulatory Commission (NRC) investigations concluded that the rust hole had been growing for at least four years and that Davis−Besse's managers had ignored the evidence because they were focused on profits rather than safety at the plant, located 30 miles east of Toledo, OH. As part of the agreement, FirstEnergy acknowledged that the government can prove that nuclear plant employees "knowingly made false representations to the NRC" at they tried to convince the commission the plant was safe to operate beyond 2001, the Justice Department said in a statement. Thursday, January 19, a federal grand jury indicted two former Davis−Besse employees and a contractor, charging them with hiding damage from federal regulators.
Source: http://www.msnbc.msn.com/id/10943739/from/RSS/

4. *January 20, Associated Press* — **Gulf petroleum interruptions continue.** The Gulf of Mexico's offshore petroleum industry is far from recovering from hurricanes Katrina and Rita, and at least one−sixth of the region's normal daily oil production will still be off line at the start of next storm season, according to the Minerals Management Service (MMS). Katrina and Rita destroyed 115 of the Gulf's 4,000 production platforms and damaged another 52, according to a report released Thursday, January 19, by MMS. The storms' combined fury also damaged 183

pipelines, including 64 classified as major. As of Thursday, only 22 had been returned to service, the MSS said. As of this week, the MMS said 396,000 of the Gulf's normal daily production of 1.5 million barrels of oil were being kept from market because of storm damage, along with 1.8 billion cubic feet of the region's normal daily production of 10 billion cubic feet of natural gas. Future repair work will be slow, the MMS projected. "For a long−term projection, approximately 255,000 barrels a day and 400 million cubic feet of gas a day will probably not be restored to production prior to the start of the 2006 hurricane season," the report said. Hurricane season begins June 1.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/20/AR2006012000934.html

5. *January 20, Independent Online (South Africa)* — **Sabotage probed at Koeberg nuclear station.** Eskom has not ruled out sabotage as a cause of one of their nuclear reactors at Koeberg in Cape Town, South Africa, having to be shut down. The controlled shutdown occurred on Christmas day after a loose bolt somehow got inside the generator of Koeberg nuclear power station's Unit 1. The bolt was meant to be attached to the outside of the generator. Eskom chief executive, Thulani Gcabashe, said at a briefing on Thursday, January 19, that an investigation was under way. The damage would take at least three months to repair. With only one of Koeberg's reactors working during these three months, the risk of power interruptions in the Cape would increase. Eskom is now shopping around nuclear power stations to try to buy a second−hand rotor and stator to repair the problem. These parts are not kept in stock by nuclear power plant manufacturers, and it would take at least a year for new parts to be made. Koeberg's other nuclear reactor is due to be refueled in March. Gcabashe said the refueling could be "stretched" by an extra two months, but this would have to be approved by the National Nuclear Regulator.
Source: http://www.int.iol.co.za/index.php?set_id=14&click_id=14&art_id=vn20060120071013263C336169

6. *January 19, Associated Press* — **Venezuela, Brazil, Argentina move forward on gas pipeline spanning much of South America.** Venezuelan President Hugo Chavez said Thursday, January 19, that Brazil, Argentina, Venezuela would move forward on a proposed natural gas network spanning much of South America, adding that the agreement heralded a new era of regional cooperation with less U.S. influence. After a three−president summit in the Brazilian capital, Chavez, Argentina's Nestor Kirchner, and Brazil's Luiz Inacio Lula da Silva confirmed plans to develop a proposed 5,000−mile natural gas pipeline. The pipeline would stretch from Caracas, Venezuela, to Buenos Aires, Argentina. It would also link to Bolivia, Paraguay, and Uruguay. Chavez predicted the pipeline would be completed within seven years. The Venezuelan president predicted no difficulty in paying for the project, estimated at $20 billion. All countries involved will help finance the project. It wasn't clear how much each country would invest, but Chavez said the investments would pay for themselves if some countries change their gasoline−powered automobiles to natural gas. According to Chavez, that shift alone would allow for a massive increase in gasoline exports by both Venezuela and Brazil. Chavez said a first draft of the proposal will be announced by Thursday, March 9.
Source: http://www.cnn.com/2006/WORLD/americas/01/19/brazil.summit.ap/index.html?section=cnn_latest

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

7. *January 21, Associated Press* — **PNC says some debit cards compromised.** PNC Bank has told authorities that some debit card accounts were compromised by suspicious activity. PNC would not specify how many Visa Gold Check Card accounts were affected except to say it was a "very small number," and also declined to disclose the amount of money involved. The suspicious activity originated overseas. The company has notified the FBI and the U.S. Postal Service. "Our accounts are continually monitored, and when we saw what we considered suspicious activity, we immediately invalidated the cards and issued new cards," PNC spokesperson Darcel Kimble said.
Source: http://www.phillyburbs.com/pb−dyn/news/103−01212006−601121.h tml

8. *January 20, Finextra* — **Investors experience Nasdaq reporting glitch.** A computer glitch at the Nasdaq stock market late Wednesday, January 18, led to the posting of incorrect stock price quotes on many of the world's financial Websites throughout Thursday, January 19. The markets were informed of the problems −− which affected mostly New York Stock Exchange (NYSE) and Amex−listed stock −− by a news alert sent late Thursday afternoon. The problem arose before the closing bell Wednesday afternoon when Nasdaq experienced a problem in submitting transactions in NYSE and Amex−listed securities to the Consolidated Tape. Approximately 81,000 trade reports were rejected from 3:39 p.m. EST through the end of the day. As a result of the failings, individual investors using popular financial sites like MSN Money or Yahoo Finance, and at some of the major online brokerages, were exposed to erroneous price information through out Thursday.
Source: http://finextra.com/fullstory.asp?id=14777

[Return to top]

Transportation and Border Security Sector

9. *January 21, Associated Press* — **Judge approves United's plan to emerge from bankruptcy.** Judge Eugene R. Wedoff of Federal Bankruptcy Court in Chicago gave final approval on Friday, January 20, to the revamping plan of United Airlines, clearing the way for it to emerge from Chapter 11 on February 1, ending one of the largest and longest airline bankruptcies in history. Wedoff said, "Three years ago, United Airlines was in danger of dying," he said. After

reorganizing under bankruptcy protection, "once again it has the potential to be a profitable investment, a reliable business partner, and a stable employer." United, a unit of the UAL Corporation, ranks second to American Airlines, part of the AMR Corporation, among domestic carriers. While United, based in Elk Grove Village, IL, has kept flying during the bankruptcy, the company that exits bankruptcy will be much leaner than the cost−heavy one that began its restructuring on December 9, 2002. UAL has cut $7 billion in annual costs, including two rounds of employee pay cuts; eliminated more than 25,000 jobs; abolished its defined−benefit pensions; and reduced its cost structure. Once the restructuring ends, the airline plans to spend on improvements. It is allocating $400 million for capital improvements like more check−in kiosks, refurbished airplane interiors, upgraded computer systems and new ground equipment.
Source: http://www.nytimes.com/2006/01/21/business/21air.html

10. *January 20, Transportation Security Administration* — **TSA announces key elements of Registered Traveler program.** The Transportation Security Administration (TSA) on Friday, January 20, announced several parameters for a nationwide private sector Registered Traveler program, including the biometrics to be used for identification purposes and the redress process for individuals who are denied access to the program. The Registered Traveler program is envisioned as a means to accelerate the screening process at participating airports for passengers who voluntarily choose to enroll in the program. As the recently announced Rice−Chertoff vision for developing new solutions that ensure the best use of new technologies and more efficient processes to improve security and facilitate travel across U.S. borders moves forward, TSA will work with the private sector providers of Registered Traveler programs to harmonize technologies and business processes with government−sponsored travel facilitation programs. Moving forward, the program will be harmonized with the Department of Homeland Security−State Department PASS System (People, Access, Security, Service), the credentialing effort announced earlier this week by Secretaries Rice and Chertoff. The Registered Traveler programs will be market−driven and offered by the private sector. Individual participation in a Registered Traveler program will be entirely voluntary, with prices established by private sector providers. TSA will mandate a core security assessment for each applicant to a Registered Traveler program.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 01a0136

11. *January 20, Department of Transportation* — **Grants to improve air service to small communities.** The U.S. Department of Transportation (DOT) on Friday, January 20, invited communities to apply for grants under a program designed to support small towns and cities working to improve their airline service. The Small Community Air Service Development Program uses federal funds to support communities working to attract or improve air service. Congress appropriated approximately $10 million for up to a total of 40 grants this year to help communities address their local air service problems, such as high fares and insufficient levels of service. This is the fifth year DOT will award grants under the program. DOT will give priority to proposals from communities that have high airfares compared to other communities, contribute financially to the project from sources other than airport revenues, have established or will establish a public/private partnership to improve their air service, submitted proposals that will benefit a broad segment of the public with limited access to the national transportation system, and will use the assistance in a timely fashion.
For additional information: http://dms.dot.gov,

Source: http://www.dot.gov/affairs/dot0506.htm

12. *January 20, Associated Press* — **NYC transit workers reject new contract.** The city's transit workers, one month to the day after they stranded seven million riders with a crippling three−day strike, voted Friday, January 20, to reject their new three−year contract by a margin of just seven votes. The workers opted to ignore Transport Workers Union (TWU) local president Roger Toussaint's call for ratification and follow the lead of a dissident group urging rejection. The final tally was 11,234 against and 11,227 in favor. The Metropolitan Transportation Authority (MTA), which oversees the city's mass transit system, had no immediate comment. Toussaint said his union was ready to "go back to the drawing board" and meet with the MTA as soon as possible. The December 20 strike by 33,000 workers, right in the middle of the holiday shopping season, shut down the nation's largest mass transit system for three days. But it was an illegal walkout, violating the state's Taylor Law and putting the union's members at dire financial risk. TWU Local 100 was already fined $3 million, while TWU workers were hit with $35 million in fines −− two days pay for each day on strike.
Source: http://www.boston.com/news/local/connecticut/articles/2006/01/20/nyc_transit_workers_vote_to_reject_new_contract/

13. *January 20, Associated Press* — **Northwest says it is unprepared for strike.** On the third day of Northwest Airlines' bid to have its union contracts tossed out by a bankruptcy court, an airline executive testified that a strike by employees would cause it to liquidate and that it has not prepared for any work stoppage. Northwest Airlines, which is asking employees for $1.4 billion in wage and benefit concessions, finished last year with nearly $300 million more in cash than its executives expected as late as October, thanks to increased revenue and cost cuts agreed to by pilots in 2004. Northwest has maintained since declaring bankruptcy that it needs wage and benefit concessions from its employees valued at $1.4 billion and without these it said it will lose $1.1 billion this year. David Davis, senior vice president of finance and controller at Northwest Airlines, did not say what the higher−than−expected cash at year−end does for the carrier's prospects of getting out of bankruptcy, nor did he say how the higher−than−expected cash impacts the carrier's outlook for losses in 2006. Asked by the pilot union's attorney if Northwest has a contingency plan for a work stoppage, Davis, who is involved with developing the carrier's operational budget, responded, "any sustained work stoppage would result ... in a liquidation of the company."
Source: http://www.usatoday.com/travel/news/2006−01−19−northwest−str ike_x.htm

14. *January 20, Seattle Times* — **Alaska isn't the only airline with ground−safety troubles.** Airline accidents on the ground are so common that aviation experts have a term for them: "ramp rash." It's hard to quantify them because reporting requirements are vague, but a panel of safety experts who studied the problem in 2004 estimated ground accidents cost the world's airlines $5 billion a year. Although several Alaska Airlines mishaps have made headlines in the past month, national and local aviation experts say accidents are a problem for all airlines. On December 26, when a ramp worker hit an Alaska Airlines MD−80 with a baggage loader. The worker failed to report the accident. Flight 536 was allowed to depart, and the small crease in the fuselage eventually ruptured into a 1−foot−by−6−inch hole, causing the cabin to depressurize at 26,000 feet. The plane returned safely to Seattle−Tacoma International Airport. Since an Alaska Airlines MD−80 was damaged by a baggage loader at Seattle−Tacoma International Airport on December 26, the Federal Aviation Administration (FAA) has received

reports of at least six similar incidents at airports around the country, including one more at Sea−Tac and one in which a worker died.
Source: http://seattletimes.nwsource.com/html/businesstechnology/200 2750657_alaska20.html

15. *January 20, Los Angeles Daily News* — **Security tighter at LAX, other sites after warning.** Hours after a new audiotape from Osama bin Laden warned of imminent terrorist attacks against the U.S., law enforcement officials in Los Angeles said they are on alert but that the city faces no known terrorist threat. "At this time there is no known direct threat to Los Angeles. But as always, we remain vigilant and encourage our residents to do the same," Mayor Antonio Villaraigosa said in a statement. As a precaution, officials beefed up security at high−profile targets such as the Port of Los Angeles, Los Angeles International Airport (LAX), and Department of Water and Power facilities, Villaraigosa said. The Los Angeles Police Department followed through with a plan to increase its presence at LAX, which was scheduled before the release of bin Laden's threat, Officer Maria Garcia said. "We're always keeping a watchful eye," Garcia said.
Source: http://www.dailynews.com/news/ci_3418741

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

16. *January 20, Agricultural Research Service* — **Prints help find where outbreaks begin.** Locating potential sources of brucellosis outbreaks is easier now, thanks to a new DNA fingerprinting technique developed by scientists with the Agricultural Research Service (ARS) and the Animal and Plant Health Inspection Service (APHIS). Finding the source of these outbreaks helps with identification and isolation of infected animals, and with telling whether the outbreaks started in wildlife. The new technique −− called "HOOF−Prints," for Hypervariable Octameric Oligonucleotide Fingerprints −− allows scientists to identify strains of brucellosis through differences in their DNA sequences, and to separate these strains into subtypes. Brucellosis is an extremely infectious disease caused by Brucella bacteria that induce abortions in many animals, including sheep, goats, cattle, pigs, elk, and bison. Brucellosis can prove costly to livestock producers through testing and losses. The new method uses polymerase chain reaction (PCR) technology, which copies large amounts of DNA molecules from small amounts of source DNA. According to Ewalt, the HOOF−Prints technique is intended to complement existing PCR and bacteriological tests used to identify Brucella species. HOOF−Prints could eventually be applied toward generating an international database of Brucella fingerprints that would be used to control the disease, according to ARS microbiologist Betsy Bricker.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

17.

January 20, Stop Soybean Rust News — **Florida soybean rust count grows to 10 counties.** A 10th Florida county −− Marion −− is now listed as positive for soybean rust on kudzu in 2006. The Marion County infection was found by the same team that scouted and found the positive locations in nine other counties which was announced on Tuesday, January 17, but was confirmed and officially reported Friday, January 20. A six person scouting team drove two vehicles for 2,500 miles around Florida from January 11 to January 13. The team's intensive scouting resulted in positive finds of soybean rust in 10 Florida counties: Polk, Duval, Leon, Alachua, Pasco, Hernando, Hillsborough, Lee, Marion, and Gadsden. Polk county was the only one of the 10 counties with no soybean rust finds in 2005. They visited all the positive kudzu rust sites from 2005 that they could find, except for the Dade County site in Miami. Of all the sites that were positive for soybean rust in 2005 and that they were able to locate (13 out of 15), nine were positive for rust in 2006 in nine counties. In addition, they observed 11 kudzu sites that were negative in 2005; one of these sites, in Polk County, is now positive in 2006.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=672

18. *January 19, Animal and Plant Health Inspection Service* — **Idaho's class free brucellosis status changed.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is amending its brucellosis regulations concerning interstate movement of cattle by changing Idaho's classification from Class Free to Class A. This action is necessary in order to prevent the spread of brucellosis. In order for a state to attain and keep their Class Free status, all cattle herds within that state must remain free of Brucella abortus for a period of 12 consecutive months. APHIS has determined that Idaho no longer meets the standards for Class Free status. Idaho was classified as Class Free until a brucellosis infected herd was discovered on November 14, 2005. On November 29, 2005, another brucellosis infected herd was confirmed. With the discovery of the second infected herd, Idaho no longer meets the standards for Class Free status. The classifications for brucellosis are as follows: Class Free, Class A, Class B, and Class C. When brucellosis is found in more than one herd of cattle in a brucellosis−free state within a two−year period, the state is downgraded to Class A status. Aside from Idaho, only two states, Wyoming and Texas, are affected with cattle brucellosis. Both states are designated as Class A.
Brucellosis information: http://www.aphis.usda.gov/vs/nahps/brucellosis/
Source: http://www.aphis.usda.gov/newsroom/content/2006/01/brufreid. shtml

19. *January 19, Wichita Eagle (KS)* — **First test shows chronic wasting disease in Kansas deer.** Preliminary tests have shown a whitetail doe shot in northwest Kansas has chronic wasting disease (CWD), a disease that has impacted deer populations in some Rocky Mountain and eastern states. Keith Sexson, Kansas Department of Wildlife and Parks (KDWP) assistant secretary, made the announcement this afternoon at the KDWP commission meeting in Kansas City, KS. It would be the first case of CWD found in a Kansas wild deer out of more than 6,000 samples tested since 1996. Kansas' only other positive test came from a domesticated elk in 2001. Kansas State University veterinarians notified Wildlife and Parks of the results Wednesday, January 18. A sample has been set to a federal veterinary lab for confirmation. Results are expected in a week. CWD information: http://www.cwd−info.org/
Source: http://www.kansas.com/mld/kansas/13664167.htm

20. *January 19, Lakeland Ledger (FL)* — **Panel will advise state's troubled citrus industry.** The Citrus Commission on Wednesday, January 18, agreed to form a blue−ribbon panel

representing all segments of Florida citrus to advise it on the industry's future. The panel also will advise the commission on what role the Florida Department of Citrus should play in that future. The Florida Citrus Commission is the department's governing body. "It won't be a nine billion dollar industry, I can tell you that," said Robert Underbrink, the chief executive officer of Consolidated Citrus LP, the state's largest grower. As Underbrink noted, the industry will be hard−pressed to keep that economic pace under pressures from citrus canker and citrus greening, two bacterial diseases that threaten to diminish fruit production, and from commercial and residential developers flashing big money to purchase grove property. The amount of grove land, and with it the supply of citrus fruit, have been diminishing rapidly under the combined pressures. While commissioners and audience members agreed on the need for the panel, they disagreed on its composition and mission. Disagreement also arose over the scope of the committee's mission. Some argued for a comprehensive study of the entire industry. But some, questioned whether the commission−sponsored committee had the authority to advise private companies and other citrus groups.
Source: http://www.theledger.com/apps/pbcs.dll/article?AID=/20060119/NEWS/601190352/1001/BUSINESS

21. *January 19, Farm & Ranch Guide* — **Forecasting system helps farmers assess scab risk.** Farmers in wheat production areas susceptible to Fusarium head blight (FHB, scab) are encouraged to use a multi−state forecasting system that can help assess disease risk and evaluate management options. The forecasting system estimates the risk of a scab epidemic with greater than 10 percent severity using weather variables observed seven days prior to flowering. Wheat is most susceptible to scab during the flowering growth stage. Weather during the pre−flowering time period influences reproduction of the fungus that causes head scab in wheat. Erick DeWolf is a plant pathologist at Penn State University involved with development of the forecasting system. He indicates that accuracy of the pre−flowering forecast is near 80 percent, based on information used to develop and test the models. However, DeWolf stresses that if weather becomes favorable for disease during the flowering or grain filling stages of growth, the model may underestimate the amount of disease. FHB or scab is regarded as one of the most serious grain diseases, which can result in wheat unsuitable for milling and barley unfit for malting.
Forecasting system: http://www.wheatscab.psu.edu
Source: http://www.farmandranchguide.com/articles/2006/01/19/ag_news/production_news/prod20.txt

[Return to top]

Food Sector

22. *January 20, Associated Press* — **Renewed Japan beef ban prompts U.S. probe.** U.S. Department of Agriculture (USDA) officials scrambled Friday, January 20, to repair a delicate beef−trading relationship after Japan discovered a shipment containing bone that Asian countries consider at risk for mad cow disease. Hours after Japan halted American beef imports, USDA Secretary Mike Johanns dispatched inspectors to Japan and sent extra inspectors to plants that sell meat to Japan. He also ordered unannounced inspections. The government barred Brooklyn, NY, based Atlantic Veal & Lamb, the plant that sent the shipment, from selling meat to Japan. Johanns said he would take action against the department inspector who

cleared the shipment. The inspector should have noticed the problem on plant documents, Johanns said. USDA officials said that for now, American beef is being held at Japanese ports until the U.S. completes a report on what happened, which Johanns intends to deliver "immediately." Johanns said he would try to reassure other Asian countries that followed the lead of Japan, which six weeks ago ended a ban on American beef imposed after the discovery of mad cow disease in the U.S. in December 2003.
Source: http://www.cbsnews.com/stories/2006/01/20/ap/business/mainD8 F8GUL00.shtml

23. *January 19, Oregonian* — **Lab tests tie E. coli to dairy's raw milk.** Laboratory analysis has conclusively linked 18 cases of E. coli illness to raw milk from the Dee Creek Farm in Cowlitz, WA, officials said Wednesday, January 18. Jerry Beundel, a food safety officer with the Washington State Department of Agriculture, said that the DNA "fingerprint" of raw milk from dairy customers, from the dairy and from samples swabbed from the cattle matched. Some patients had started antibiotics when tested because of a delay in identifying dairy customers involved in the outbreak, Denny said. Cultures from them were inconclusive, but those cases matched key symptoms from other dairy customers. Five patients were hospitalized; the other 13 reported distinctive symptoms such as bloody diarrhea. Victims were from Clark and Cowlitz counties in Washington, and Clatskanie in Columbia County, Oregon.
Source: http://www.oregonlive.com/metronorth/oregonian/index.ssf?/base/metro_north_news/1137698723236880.xml&coll=7

[Return to top]

Water Sector

24. *January 22, Salt Lake Tribune (UT)* — **Thirty−two Utah water systems won't meet arsenic standard.** Most Utah drinking water systems, like those nationwide, are prepared to meet the U.S. Environmental Protection Agency's new arsenic limits that go into effect Sunday, January 22. Although a measurement of 50 parts per billion (ppb) of arsenic in drinking water used to be allowed, 10 ppb is considered safe under the new regulation. The change has tested the bank accounts and management ingenuity of water districts nationwide. In recent months, 32 water districts in Utah have received extensions that allow them up to three years more to solve their arsenic problems. Some water systems have shut down high−arsenic sources. Others are blending water from low−arsenic wells with water from those with higher readings. Three have built or adapted tools to capture arsenic before water is piped to customers. The moves are all geared toward removing a contaminant that is naturally occurring and that leaches into groundwater from the surrounding rock.
Source: http://www.sltrib.com/utah/ci_3426714

25. *January 21, Times Herald (MI)* — **Automatic spill detection for water plants moves ahead.** A first−of−its−kind network of chemical monitors could soon be protecting Michigan's drinking−water plants. Nearly instantaneous detection of chemical spills to the St. Clair River and Lake St. Clair could be possible this year. The monitoring system ties together three projects that would monitor 11 drinking−water plants in three counties that serve about 3.5 million people. Local officials began pushing for the system after a series of spills from plants in Sarnia, Canada. The Port Huron, Marysville, Marine City, East China Township, Ira Township, New Baltimore, and Mount Clemens water−treatment plants will get automated

equipment to continually monitor the relative acidity of the water coming through their intake pipes. Additionally, more sophisticated equipment would be installed at St. Clair, Algonac, Mount Clemens, and Detroit. Those devices would test for more than 700 chemical contaminants every 10 to 15 minutes. Both types of monitors would sound alarms to alert water−plant operators if contamination is discovered. Plant operators would have the option of shutting down their pumps then, rather than wait for late or no notice from the pollutant's source. Each of the monitors would communicate with the others in the system, and the data would be automatically uploaded to a Website.
Source: http://www.thetimesherald.com/apps/pbcs.dll/article?AID=/20060121/NEWS01/601210303/1002

26. *January 19, Inquirer (Philippines)* — **Bottled water now part of U.S. arsenal versus terror.** U.S. troops in Mindanao, Philippines, have started to use bottled water as another tool in their anti−terror campaign aimed at stamping out the Abu Sayyaf. At a press conference held at the Southern Command on Tuesday, January 17, U.S. Embassy personnel and American military officials distributed samples of the new anti−terror instrument, with accessories in the forms of leaflets bearing profiles of wanted terrorists and corresponding rewards for their capture. The label on the product, which comes in 12 oz plastic bottles, bears photos of the most−wanted Abu Sayyaf leaders −− Isnilon Hapilon, Khadaffy Janjalani, and Jainal Antel Sali Jr., alias Abu Sulaiman −− with corresponding rewards of up to five million dollars for their capture. Also printed on the label were the words “Wanted for murder, extortion, and kidnapping” and hotline numbers that informants could use to contact the appropriate agencies.
Source: http://news.inq7.net/breaking/index.php?index=2&story_id=63445

[Return to top]

Public Health Sector

27. *January 21, Agence France−Presse* — **Indonesia's bird flu death toll rises to 14.** Indonesia's confirmed death toll from the H5N1 bird flu virus rose to 14, while three patients suspected of carrying the virus were being treated in hospital, health officials said. Two siblings from Indonesia's West Java died last week and tests by a World Health Organization (WHO)−accredited laboratory showed they were infected with the H5N1 strain, health ministry official Hariyadi Wibisono said. "The results from Hong Kong arrived earlier today (Saturday, January 21) and confirmed that the two had died of bird flu," he said. Wibisono said the pair, aged four and 13, were residents of Indramayu −− site of the fifth cluster case in Indonesia, the world's fourth most populous nation −− and were in contact with dead chickens near their home. Their 15−year−old sister tested negative to initial tests but these were being repeated, an official said. Cases are tested locally and positive results, which are usually reliable, are then sent to Hong Kong for formal verification. The teenager and her 43−year−old father, who is also suspected of carrying the virus, have been moved from West Java to Sulianto Saroso hospital in Jakarta, Indonesia's main treatment center for the virus, Wibisono said.
Source: http://news.yahoo.com/s/afp/20060121/wl_asia_afp/healthfluindonesia_060121204940;_ylt=AnNjsGvp2p7kf8iAqSq5V6qJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

28.

January 20, Associated Press — **Hantavirus case confirmed.** North Dakota has its eighth−ever confirmed case of hantavirus, and the first in six years. The case was diagnosed in a woman in Grand Forks, who is recovering. Hantavirus is a severe respiratory infection spread by rodents. State Health Department disease specialist Kirby Kruger says the first cases of hantavirus in North Dakota were diagnosed in 1993. Officials later determined there had been cases dating back to the late 1970s. Two cases were reported in 2000.
Hantavirus information: http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm
Source: http://www.kfyr.com/cc−common/mainheadlines2.html?feed=12127 7&article=382173

29. *January 20, Reuters* — **Bird flu virus survives for days in droppings.** The H5N1 avian influenza virus can survive for more than a month in bird droppings in cold weather and for nearly a week even in hot summer temperatures, the World Health Organization (WHO) said in a factsheet on Friday, January 20. The new factsheet incorporates the most recent findings on the avian flu virus, which WHO says is causing by far the worst outbreak among both birds and people ever recorded. It has been found from South Korea, across Southeast Asia, into Turkey, Ukraine and Romania. It has infected 149 people and killed 80, according to the WHO figures, which do not include the most recent deaths and infections in Turkey. Bird droppings may be a significant source of its spread to both people and birds, the WHO said. "For example, the highly pathogenic H5N1 virus can survive in bird feces for at least 35 days at low temperature (four degrees C or 39 degrees F)," the WHO said. "At a much higher temperature (37 degrees C or 98.6 degrees F), H5N1 viruses have been shown to survive, in fecal samples, for six days."
WHO factsheet: http://www.who.int/csr/disease/avian_influenza/avianinfluenza_factsheetJan2006/en/index.html
Source: http://reuters.myway.com/article/20060121/2006−01−21T010344Z_01_N20130277_RTRIDST_0_NEWS−BIRDFLU−WHO−FACTS−DC.html

30. *January 20, Wall Street Journal* — **New, virulent staph infection sparks health fears.** Identified in 1999, community−associated methicillin−resistant staphylococcus aureus (CA−MRSA) is resistant to drugs and is highly virulent. It is responsible for 60 percent of all skin and soft−tissue infections treated in U.S. emergency rooms. The germ can penetrate bones and lungs, and the abscesses it causes often require surgery. In severe cases, up to a quarter of patients die. Public−health officials see a silent epidemic on the rise. Almost one percent of the population, or more than two million people, carry drug−resistant staph without symptoms. Carriers can spread the disease and suddenly become ill themselves. Public health officials blame the heavy use of antibiotics, which kill off a disease's sensitive strains and leave the field open for its hardier cousins. Staph in its common form is a bacterium carried harmlessly by nearly one−third of the U.S. population. Drug−resistant forms emerged decades ago in hospitals. Until recently, they afflicted mostly elderly or sick patients with compromised immune systems. But CA−MRSA has a distinct package of resistance genes. CA−MRSA can't always be reversed by antibiotics. It produces a poison that kills white blood cells used to fight infection and destroys the body's tissue. Especially alarming to doctors, the strain is circulating in the broad community, striking healthy patients often seemingly at random.
CA−MRSA information: http://www.cdc.gov/ncidod/dhqp/ar_mrsa_ca.html
Source: http://www.azcentral.com/health/news/articles/01200121staph. html

31. *January 20, Science* — **Sampling the antibiotic resistome.** Soil−dwelling bacteria produce and encounter a myriad of antibiotics, evolving corresponding sensing and evading strategies.

They are a reservoir of resistance determinants that can be mobilized into the microbial community. Researchers isolated a morphologically diverse collection of spore−forming bacteria from soil samples originating from diverse locations. Strains that resembled actinomycetes both morphologically and microscopically were serially subcultured to apparent homogeneity. Amplification and sequencing of 16S ribosomal DNA from a subset of strains indicated that they belonged to the actinomycete genus Streptomyces, whose species synthesize over half of all known antibiotics. Researchers constructed a library of 480 strains that was subsequently screened against 21 antibiotics. The antibiotics encompassed all major bacterial targets and included drugs that have been on the market for decades as well as several that have only recently been clinically approved. Without exception, every strain in the library was found to be multi−drug resistant to seven or eight antibiotics on average, with two strains being resistant to 15 of 21 drugs. Reproducible resistance to most of the antibiotics, regardless of origin, was observed, and almost 200 different resistance profiles were seen. Several antibiotics were almost universally ineffective against the library.
Source: http://www.sciencemag.org/cgi/content/full/sci;311/5759/374

[Return to top]

Government Sector

32. *January 20, Ledger Independent (KY)* — **Bomb threat at Bracken courthouse halts justice.** A bomb threat cleared the Bracken County Courthouse and sent defendants, attorneys, the judge and courthouse staff into the streets of Brooksville, KY, Friday morning, January 20. At about 9:40 a.m. CST, assistant circuit court clerk Libby Estill answered the phone in the clerk's office. "There was a beep sound, then an elderly−sounding female voice said, in a slow careful tone "This is a warning there are six bombs… in the courthouse." Evacuation of the entire building, including the Bracken County Sheriff's Office and other county offices took about five minutes, said Free. More than half a dozen Kentucky State Police (KSP) officers were called to assist Bracken County Sheriff Mike Nelson with a search of the building. As they began a search of building, KSP asked for radio silence; electronics can activate other electronic devices or detonate a bomb. The initial sweep included accessing the roof of the building, checking for secured windows and any indications of something out of the ordinary, said police. Following the all clear, people who had been in the courtroom were told that court proceedings would resume at 2 p.m.
Source: http://www.maysville−online.com/articles/2006/01/20/local_ne ws/016bomb.txt

[Return to top]

Emergency Services Sector

33. *January 20, The Daily Inter Lake (MT)* — **High marks for disaster drill.** Emergency−services and government agencies in Flathead County, MT, tested their response capability Wednesday, January 18. The scenario for the surprise table−top drill involved heavy snowpack and record rains caused massive cracks in Hungry Horse Dam, leading to a failure. Responders were notified of the impending disaster on the Friday before the Memorial Day holiday weekend. The dam would fail on Sunday, giving officials 48 hours to put their plan in

action. In addition to preparing an incident action plan for a dam failure, agencies were directed by Gov. Brian Schweitzer to develop a large−scale housing plan for 75,000 evacuees, using facilities in Idaho and Washington if needed, and develop a plan for restoring public services. The drill helped pinpoint potential problems with communications and challenges that would accompany such a widespread evacuation. Pete Wingert, patrol commander for the Flathead County Sheriff's Department, said work still needs to be done to determine how the county's population is spread out through the valley. The governor's office issued a press release Thursday, noting that jurisdictions involved will submit reports for review.
Press release: http://www.ideas.mt.gov/news/pr.asp?ID=276
Source: http://www.dailyinterlake.com/articles/2006/01/20/news/news0 2.txt

[Return to top]

Information Technology and Telecommunications Sector

34. *January 20, IDG News Service* — **Hacker computer networks getting harder to find.** Hacked computer networks, or botnets, are becoming increasingly difficult to trace as hackers develop new means to hide them, says security experts. Botnets are used to send spam, propagate viruses, and carry out denial of service attacks. Extortion schemes are frequently backed by botnets, and hackers are also renting the use of armadas of computers for illegal purposes through Web advertisements, said Kevin Hogan, senior manager for Symantec Security Response. Three or four years ago, it was easier to connect to botnets and estimate the size of one by noting the number of IP addresses on the network, he said. As legislation emerged cracking down on spammers, those who ran botnets started pursuing more clandestine ways to continue their operations. Rather than deter hardcore spammers, it drove them further underground, said Mark Sunner of MessageLabs. Botnets have an ebb and flow similar to biological behavior, Sunner said. Viruses on an infected computer may download new variants in an attempt to evade anti−virus sweeps. Law enforcement authorities have become more adept at tracking down botnet admins. However, the admins have countered by sticking to smaller groups of around 20,000 machines that are less likely to be detected as quickly, Sunner said.
Source: http://www.techworld.com/security/news/index.cfm?NewsID=5205 &Page=1&pagePos=4&inkc=0

35. *January 19, Secunia* — **F−Secure anti−virus archive handling vulnerabilities.** Some vulnerabilities have been reported in various F−Secure products, which can be exploited by malware to bypass detection to compromise a vulnerable system. A boundary error in the handling of ZIP archives can be exploited via a specially crafted ZIP archive to cause a buffer overflow and execute arbitrary code. In addition, an error in the scanning functionality when processing RAR and ZIP archives can be exploited to prevent malware from being detected. Secunia reports that a patch can be obtained at the vendor website.
Patch: http://www.f−secure.com/security/fsc−2006−1.shtml
Source: http://secunia.com/advisories/18529/

36. *January 19, Securiteam* — **Oracle database and report engine multiple vulnerabilities.** Lack of proper input validation in Oracle Database and Report engine allows attackers to cause SQL injection, directory traversal, gather authentication information and overwrite arbitrary files.

Vulnerable systems include Oracle 10g Release 1, Oracle Database 10g Release 2, Internet Application Server; Oracle Application Server, and Oracle Developer Suite.
Source: http://www.securiteam.com/securitynews/5UP0B2KHFY.html

37. *January 19, FrSIRT* — **CheckPoint VPN−1 SecureClient Local Privilege Escalation vulnerability.** A vulnerability has been identified in CheckPoint VPN−1 SecureClient, which could be exploited to obtain elevated privileges. This flaw is due to a design error in the "SR_Watchdog.exe" file that launches the GUI process (SR_GUI.exe) using the "CreateProcess()" function with a NULL "pApplicationName" parameter, which could be exploited by local attackers to create an environment where a malicious program will be executed with the privileges of the user running the vulnerable application. Affected products include CheckPoint VPN−1 SecureClient. FrSIRT reports that it is not aware of any official supplied patch for this issue.
Source: http://www.hackerscenter.com/archive/view.asp?id=22074

38. *January 19, Security Focus* — **WebspotBlogging Login.PHP SQL Injection vulnerability.** WebspotBlogging is prone to a SQL injection vulnerability. This issue is due to a failure in the application to properly sanitize user−supplied input before using it in an SQL query. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. Security Focus is not aware of a patch.
Source: http://www.securityfocus.com/bid/16319/discuss

39. *January 19, BBC News* — **Zombie PCs target vulnerable sites.** Recently, denial−of−service (DoS) attacks by criminals who recruit so−called zombie PCs and use their net addresses to deluge sites with data, have become increasingly more prevalent. According to security firm CipherTrust, high profile websites are ripe for this cyber−crime, largely due to the ease with which attacks can be launched. Criminals intent on bringing down sites recruit mostly Windows PCs by infecting them with viruses or worms. They then use the net addresses of these zombie PCs to deluge targeted websites with a huge amount of data, causing the servers to fall over and forcing the website offline. CipherTrust has seen an alarming rise of nearly 50 percent in the number of infected machines being recruited over the past six months. The middlemen in these attacks tend to be home users. This is largely a result of the Sober virus which hit PCs around the world at last year. It estimates that 250,000 new machines are infected every day. "China has the most zombie PCs at the moment and the U.S. is regularly number two, with Germany at number three and the UK, with just three percent of infected machines, at number 10," said David Stanley, managing director of CipherTrust.
Source: http://news.bbc.co.uk/1/hi/technology/4625304.stm

40. *January 18, Securiteam* — **Mozilla Thunderbird attachment spoofing vulnerability.** Mozilla Thunderbird displays display attachments in a wrongful manner which allows attackers to spoof attachments and convince users to execute arbitrary programs. The vulnerability is caused due to attachments not being displayed correctly in mails. This can be exploited to spoof the file extension and the associated file type icon via a combination of overly long filenames containing white spaces and "Content−Type" headers not matching the file extension. Successful exploitation may lead to malware being saved to the desktop. Vulnerable systems include Mozilla Thunderbird versions 1.0.2, 1.0.6, and 1.0.7; Mozilla Thunderbird version 1.5

is immune.
Source: http://www.securiteam.com/windowsntfocus/5CP0J2KHFO.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a public exploit for a vulnerability in VERITAS NetBackup Volume Manager Daemon (vmd). The VERITAS NetBackup vmd listens on network port 13701/tcp. An attacker could send a specially crafted packet to the Volume Manager on a vulnerable system to cause a buffer overflow or a denial of service condition. Successful exploitation may allow may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system with root or SYSTEM privileges. More information about this vulnerability can be found in the following URL:

VU#574662 VERITAS NetBackup library buffer overflow vulnerability:
http://www.kb.cert.org/vuls/id/574662

US−CERT strongly encourages users and administrators to review the following mitigation to address this vulnerability as soon as possible:

Review the Symantec Advisory SYM05−024 and apply the recommended updates to address this vulnerability:

http://seer.support.veritas.com/docs/279553.htm

http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNL OAD.htm

Restrict access to the ports used by the NetBackup services.

Malicious Website Exploiting Sun Java Plug−in Vulnerability US−CERT is aware of an active malicious website that exploits a vulnerability in the Sun Java JRE. The initial report led US−CERT to believe the website was exploiting VU#974188. After further analysis, it was determined that the actual vulnerability being exploited was VU#760344. This vulnerability allows a Java Applet to bypass java security settings. Once these checks are bypassed, a remote attacker may be able to exploit this vulnerability to execute arbitrary code on the host machine. More information about these vulnerabilities can be found in the following URL:

VU#760344 Sun Java Plug−in fails to restrict access to private Java packages:
http://www.kb.cert.org/vuls/id/760344

VU#974188 Sun Java Runtime Environment "reflection" API privilege elevation vulnerabilities: http://www.kb.cert.org/vuls/id/974188

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 65535 (Adoreworm), 139 (netbios−ssn), 41170 (−−−), 80 (www), 32768 (HackersParadise), 113 (auth) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

41. *January 21, KESQ Channel 3 (CA)* — **Desert Sands Unified increases security at local schools.** California's Desert Sands Unified School District is beefing up security by installing surveillance cameras at three Indio schools. The cameras will go in at Amistad High School, Wilson Middle School, and Eisenhower Elementary. Ideally, schools are places where kids can feel safe as they learn. But too often, Valley schools have been targets of vandalism and theft. That's why the Desert Sands Unified School District is spending around $74,000 to install security cameras. Principals at those schools say it's worth it. "Computers, projectors, when those are stolen we're at a loss, because that affects teaching and our students learning." Amistad will be the fourth high school in the district to have security cameras. Because Wilson and Eisenhower are located nearby, they'll be using the same system. Parents we talked with say installing cameras is a great idea, not only to protect school property, but children as well. District officials plan to have the system up and running within the next several months.
Source: http://www.kesq.com/Global/story.asp?S=4386463&nav=9qrx

[Return to top]

General Sector

42. *January 20, Denver Post (CO)* — **Eleven indicted in eco−terror investigation.** Members of an Oregon−based group of eco−terrorists who called themselves "the family" were indicted for a cutting a swath of destruction across the western U.S. The federal indictment, unsealed Friday, January 20, tells a story of 4 1/2 years of vandalism and fire bombings. It contends that 11 suspects were responsible for 17 incidents in California, Colorado, Oregon, Washington, and Wyoming. "In all, their trail of destruction across the Pacific Northwest and beyond resulted in millions of dollars of property damage," U.S. Attorney General Alberto Gonzales said in a prepared statement.
Source: http://www.denverpost.com/news/ci_3421918

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact DHS

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

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

Department of Homeland Security Disclaimer