Department of Homeland Security Daily Open Source Infrastructure Report for 27 January 2006

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

Daily Highlights

- CBC News reports American law enforcement officials are accusing a Quebec man of laundering hundreds of millions of dollars −− illicit moneys from narcotics, stock fraud, or tax evasion −− and changing that money into other funds by wire transfers. (See item 8)
- The Associated Press reports the Department of Homeland Security has decided to try a modernized siren alert system in the Washington, DC, metro area, since new high−tech systems still aren't enough to alert millions of area residents. (See item 33)

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 26, Associated Press* — **Inspector general faults controls over Lawrence Livermore badges.** There are inadequate controls over security badges at Lawrence Livermore National Laboratory, according to a report Wednesday, January 25, by the Energy Department's inspector general. The report said that of 1,261 employees with security badges who left the University of California−run research and nuclear weapons lab from 2002−2004, 373 did not turn in their badges before leaving as required. Eleven badges were categorized as "accounted for" when they were lost or stolen. Inspectors also sampled 140 employees who left the lab and found that three−dozen retained their Livermore security access authorizations for 10 to 60 days

after their departure date, and others did not follow proper procedures for security termination briefings or processing. "...any failure to properly control security badges and clearance terminations for departing Livermore employees has the potential to degrade the department's security posture," said the report, which recommended better internal controls at the lab including improvements to how badges are retrieved and the Energy Department is notified about security access termination. Michael Kane, an associate administrator at the Energy Department's National Nuclear Security Administration, said "We are aware that this inspection, and subsequent results, are similar to results identified previously at Los Alamos National Laboratory."
Source: http://www.pe.com/ap_news/California2/CA_Lawrence_Livermore_Security_222015CA.shtml

2. *January 25, Agence France−Presse* — **Plutonium monitor could help combat proliferation.** U.S. scientists are testing a prototype device that could help detect whether a country is secretly harvesting plutonium from its nuclear program with the goal of making a nuclear bomb. The device could help combat proliferation of weapons−grade plutonium among states that turn to nuclear power in the coming decades to meet their energy needs, the report in the next New Scientist says. But it is still being tested and thus cannot be used to defuse the present row embroiling Iran, which Western countries suspect is trying to build a bomb. And if it works, it still could not thwart states that refuse deals with nuclear inspectors or hide their reactors, it says. The detector built by researchers at Lawrence Livermore National Laboratory in California counts antineutrinos. If more plutonium is being produced than expected, the number of these high−energy particles will fall at a higher rate as more uranium is burned up. Scientists in France and Brazil are also building their own prototypes. The invention would not help measure the output of countries that refuse to have their facilities monitored, do not declare their reactors, or press ahead with building a nuclear bomb using enriched uranium rather than plutonium.
Source: http://news.yahoo.com/s/afp/20060125/sc_afp/irannuclearpolit ics_060125192007

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *January 26, Burlington County Times (NJ))* — **School, homes, bank evacuated after gas line hit in New Jersey.** The Walnut Street Elementary School, four nearby homes and a bank in Delanco, NJ, were evacuated Wednesday, January 25, after a contractor accidentally punctured an underground natural−gas pipe, police said. No injuries were reported, police said. Workers demolishing a wall and a concrete walkway at the school struck a gas main with a backhoe at about 1 p.m. EST, school principal Dorothy Mongo said. The school was immediately evacuated, along with four homes within a one−block radius of the rupture and the Delanco Savings Bank on Burlington Avenue, police said. Police officers and firefighters temporarily closed Burlington Avenue and Walnut Street near the accident. Some 100 students were evacuated in about five minutes, Mongo said. They were taken to the nearby Pearson Elementary School on Burlington Avenue. Public Service Electric & Gas Co. crews shut off the gas main by 1:30 p.m. EST. A short time later, residents who had been evacuated were permitted to return to their homes and the bank reopened. Walnut Street Elementary School remained closed until Thursday, January 26.

Source: http://www.phillyburbs.com/pb−dyn/news/112−01262006−603629.h tml

[Return to top]

Defense Industrial Base Sector

4. *January 25, Global Security Newswire* — **Report encourages Pentagon to focus more on homeland defense.** The military needs increased focus on unconventional warfare and defense against nuclear and biological weapons, and less on developing certain advanced conventional weaponry, according to the report, "Restoring American Military Power, a Progressive Quadrennial Defense Review," by the Center for American Progress, released Tuesday, January 24. The review is intended to provide a counter−vision for the much−anticipated Defense Department Quadrennial Defense Review expected to soon be released. The group's report advocates cutting development and production of eight major weapons types: the F−22 fighter, Virginia class submarine, DD(X) Destroyer, V−22 Osprey, C−130J transport aircraft, offensive space−based weaponry, further deployment of the U.S. national missile defense system; and "obsolete and unnecessary elements of the nuclear posture." The weapons are costly but unnecessary, providing little additional advantage over other existing systems, according to the report. The report advocates doubling Pentagon expenditures on homeland defense to "at least $20 billion" annually, to increase its capacities to support civil authorities following unconventional and high−explosive attacks or other incidents. The report also advocates abandoning development of a new earth penetrating nuclear weapon capability, maintaining a "surge capacity" for building additional warheads if needed, and continuing the administration's Reliable Replacement Warhead program.
Report: http://www.americanprogress.org/atf/cf/%7bE9245FE4−9A2B−43C7 −A521−5D6FF2E06E03%7d/QDR.PDF
Source: http://www.nti.org/d_newswire/issues/2006_1_25.html

[Return to top]

Banking and Finance Sector

5. *January 26, Reuters* — **First Data to spin off Western Union.** First Data Corp., the world's largest electronic and payment services processor, said it will spin off its Western Union money transfer business to shareholders but keep its struggling U.S. credit card issuing business. First Data said it would divest Western Union through a tax−free spin−off, creating an independent, publicly traded company focused on consumers. First Data plans to strengthen its U.S. card business, which has been its weakest performer, weighing down its payments and merchant businesses, but will look at selling other underperforming units within the company. Analysts said the spin−off made sense as the parts of First Data were worth more than the whole and leaving First Data's card and merchant businesses together available for continued cross−selling and operational synergies. Chief Executive Ric Duques said the company expects to complete the spin−off in the second half and will update shareholders when it reports first−quarter results in April. Following the deal, Denver−based First Data said it would reorganize into three divisions −− financial institution services, commercial services and international.
Source: http://www.nytimes.com/reuters/business/business−financial−f irstdata.html?_r=1

6. *January 26, Associated Press* — **Ameriprise notifies clients of data theft.** Ameriprise Financial Inc. said Wednesday, January 25, it has notified about 226,000 people that personal data were stored on a laptop computer that was stolen from an employee's vehicle. Ameriprise said it has alerted 68,000 current and former financial advisers whose names and Social Security numbers were also stored on the same computer. About 158,000 clients had only their names and internal account numbers exposed. Ameriprise said it had received no reports that the data lost in the theft had been used improperly. Ameriprise said the theft appeared to be a "random criminal act" and that it has been working with law enforcement to recover the laptop, which it said was stolen from an employee's locked vehicle that was parked offsite. Company spokesperson Steve Connolly said the laptop was stolen in late December outside Minnesota, but he declined to say where. Ameriprise said there was no other client−identifying information on the computer such as Social security numbers, addresses, phone numbers, or birth dates. Client accounts could not be accessed with the information that was stored on the computer because Ameriprise does not allow access via account numbers alone without additional personal information provided only by the client.
Source: http://www.newsobserver.com/24hour/business/story/3107334p−1 1809964c.html

7. *January 25, Gannett* — **Identity theft, money target of con game.** Scam artists are targeting Ohio residents with an unclaimed funds ruse. The Ohio Department of Commerce's Division of Unclaimed Funds issued an identity theft alert Tuesday, January 24 after receiving numerous complaints from residents throughout the state. Potential victims receive a letter or telephone call from an organization calling itself the "Department of Unclaimed Funds," located on West Fifth Avenue in Columbus, OH, telephone 1−800−467−7010. The individuals writing the letters and making the calls are using various names including Brian Green, Fernando, and Amy. The scammers are also using a Sacramento, CA address and the name of David Reynolds. "The so−called 'Department of Unclaimed Funds' is not a government entity and has no relationship to the Ohio Division of Unclaimed Funds or any other State of Ohio agency," Unclaimed Funds Superintendent David Moore stated. This organization is informing Ohioans that they have unclaimed funds to be claimed and asks for a credit card number to charge $80 to receive a claim form. The organization also has asked for copies of drivers' licenses and Social Security cards.
Source: http://www.centralohio.com/apps/pbcs.dll/article?AID=/BE/200 60125/NEWS01/601250307/1002&template=BE

8. *January 25, CBC News (Canada)* — **Quebec man accused of laundering millions.** American law enforcement officials are accusing a Quebec man of laundering hundreds of millions of dollars. Drug enforcement officials say Martin Tremblay, 43, laundered amounts of money that would rival the operations of some Columbian drug cartels. Officers had been keeping an eye on Tremblay and his company Dominion Investments for nearly three years. The man may have been laundering money for longer than three years, said special agent Christopher Giovino of the U.S. Drug Enforcement Administration. "He is charged with taking in illicit moneys from narcotics or stock fraud or tax evasion, and changing over that money into other funds by wire transfers," Giovino said. Giovino alleges Tremblay would then deposit that money, once laundered, into special accounts for customers. Investigators allege Tremblay would collect a commission for his efforts, and that he laundered as much as $1 billion. Tremblay not only ran a brokerage house in the Bahamas, but was also the head of a Swiss bank in Nassau. In addition

to heading up the Dominion Investment brokerage house since 1994, Tremblay also ran the Nassau branch of Ferrier Lullin since 2005. Ferrier Lullin is one of the most important Swiss banks in Bahamas' capital city.
Source: http://www.cbc.ca/montreal/story/qc−launder20060124.html?ref =rss

9. *January 25, WTOP (MD)* — **Maryland residents warned of new identity theft scam.** Maryland officials are warning residents about a new phone scam. Attorney General Joe Curran says people posing as Maryland Health Department employees ask residents to verify their name, address, and bank account information in order to claim at $1,000 prize from the Health Department. "The Maryland Health Department is not calling people offering prizes. Government agencies don't do that," he says. The same con artists have been scamming people in a dozen states, according to other Attorney's General offices. Residents in other states have received calls where a person claiming to be from the Health Department informs them that they are eligible for medical discount vouchers. The callers claim to already have the resident's personal information −− including address, name of their bank and bank account routing number −− and then ask the caller to "verify" their identity by reciting their checking account number.
Source: http://www.wtopnews.com/?nid=25&sid=679597

10. *January 25, Federal Trade Commission* — **Federal Trade Commission releases Top 10 consumer fraud complaint categories; identity theft leads the list.** On Wednesday, January 25, the Federal Trade Commission released its annual report detailing consumer complaints about fraud and identity theft in 2005. Complaints about identity theft topped the list, accounting for 255,000 of more than 686,000 complaints filed with the agency in 2005. The complaints, filed online or at a toll−free number, are shared via a secure database with more than 1,400 federal, state, and local law enforcement agencies, and law enforcement and consumer protection agencies in Canada and Australia. Identity theft complaints represented 37 percent of the 686,683 complaints filed. Other findings from the report include: Internet−related complaints accounted for 46 percent of all fraud complaints; the percent of Internet−related fraud complaints with “wire transfer” as the reported payment method more than tripled between 2003 and 2005; credit card fraud was the most common form of reported identity theft, followed by phone or utilities fraud, bank fraud, and employment fraud; the most frequently reported type of identity theft bank fraud was electronic funds transfers; the major metropolitan areas with the highest per capita rates of reported identity theft were Phoenix/Mesa/Scottsdale, AZ; Las Vegas/Paradise, NV; and Riverside/San Bernardino/Ontario, CA.
Consumer Fraud and Identity Theft Complaint Data:
http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf
Source: http://www.ftc.gov/opa/2006/01/topten.htm

11. *January 25, Finextra* — **Financial Services Sector Coordinating Council warns U.S. banks to plan for bird flu pandemic.** The U.S. Financial Services Sector Coordinating Council (FSSCC) has issued a paper warning banks that their current business continuity measures may not be adequate for dealing with a widespread outbreak of bird flu. The council says a possible avian influenza pandemic poses a "unique threat" to the industry and is calling on banks to re−examine current contingency plans. The FSSCC says bird flu could cause problems for the industry that are distinct from the issues posed by disruptions associated with natural disasters or deliberate malicious activity. For example, a widespread bird flu epidemic is likely to affect

multiple regions of the country and the world at the same time, so the backup facilities that banks have established −− even remote sites hundreds of miles distant from primary facilities −− may be just as afflicted as primary locations. Donald Donahue, chairman of the FSSCC says that continuity planning needs to encompass the long−term and large−scale disruptions. Reviews should include factors such as the splitting and segregating of critical staff into separate locations, expanded telecommuting, and the use of teleconferencing to avoid travel. The World Health Organization is expected to advise companies to plan for 25 percent absence.
Paper: http://www.fsscc.org/index.html.
Source: http://finextra.com/fullstory.asp?id=14802

12. *January 25, KPTV−12 (OR)* — **Computer records of more than 300,000 Providence patients stolen.** Some 365,000 patients who received health care through Providence Hospitals' home care system are being warned of possible identity theft after the theft of computer records. According to Providence, there is no evidence that the stolen information has been used by identity thieves. According to the heath care provider, the theft only affects those patients of Providence Home Services. Providence is currently contacting patients who were affected by the theft. The company said the stolen data includes Social Security numbers, clinical, and demographic information. According to the heath care provider, in a small number of cases, some patient financial data was stolen. Providence says the stolen data was on computer backup disks and tapes in a case that was stolen from the car of an employee. The theft was reported on December 31, 2005. The company says it is working with local law enforcement and the FBI. According to Providence, the duplicate data sources were taken home nightly by designated employees as part of a backup process intended to guarantee access to critical information in case of an emergency at our primary offices. Providence believes the thief would need specialized computer skills to access the data.
Source: http://www.kptv.com/global/story.asp?s=4411046&ClientType=Pr intable

13. *January 25, Government Computer News* — **Agencies need to improve, share money−laundering data.** The Department of Treasury released the first governmentwide analysis of money laundering and terrorist financing weaknesses that criminals and terrorists exploit through a variety of techniques. What the analysis determined was that additional data needs to be collected in a more consistent way across agencies to help stem the flow of illicit funds. The laundering methods include well−established techniques for integrating dirty money into the financial system through banks, as well as innovations that exploit global payment networks through money transmitters, online payment systems, stored−value cards, and informal value transfer systems such as unregulated international financing networks called halawas. Sixteen agencies and bureaus collaborated on the U.S. Money Laundering Threat Assessment, released earlier this month. The analysis revealed that agencies' data is not as developed as it should be, and not collected in a systematic way across government. Agencies have developed tracking systems that are tailored to meet their individual needs and are incompatible with other systems. Problems include data fields are collected by some but not all agencies, differences in definitions, and duplications. Currently, it is not possible to estimate with accuracy the total amount of money laundering activity that federal law enforcement captures.
Report: http://www.ustreas.gov/offices/enforcement/pdf/mlta.pdf
Source: http://www.gcn.com/vol1_no1/daily−updates/38092−1.html

[Return to top]

Transportation and Border Security Sector

14. *January 26, Associated Press* — **Inactive grenade grounds Northwest flight attendant.** A Northwest Airlines flight attendant has been grounded and could face charges after security personnel found a real but inactive hand grenade in her carry−on luggage, officials said Wednesday, January 25. The 39−year−old Cordova, TN, woman, whose name was not released, was expected to appear Thursday in Milwaukee County Circuit Court. She had been scheduled to work on a Milwaukee−to−Detroit flight Tuesday morning, January 24, when federal Transportation Security Administration (TSA) officers detected the inert grenade in her baggage at Mitchell International Airport, said Kim Brooks, a spokesperson for the Milwaukee County Sheriff's Department. The attendant told the deputies that she purchased the grenade at an Army surplus store as a present to bring home for her son, Brooks said. She could be charged with disorderly conduct and also could face a federal fine of up to $1,500, according to Brooks and TSA spokesperson Lara Uselding.
Source: http://www.usatoday.com/travel/flights/2006−01−26−grenade−at tendant_x.htm

15. *January 26, Department of Transportation* — **Work to repair highway and rail bridges over St. Louis Bay making progress.** Work to rebuild the bridges over St. Louis Bay, MS, is reaching “critical mass” according to Department of Transportation Secretary Norman Y. Mineta who arrived in Gulfport, MS, Thursday, January 26, for a progress report on hurricane recovery efforts. Mineta took a train ride over the repaired CSX railroad bridge and then boarded a U.S. Coast Guard vessel for a close−up look at the devastated U.S. 90 highway bridge. He reviewed plans to begin construction on a replacement to that span. The railroad bridge will open in early February, with work to begin on the U.S. 90 crossings over St. Louis Bay and Biloxi Bay as soon as possible, Mineta said. Mineta said his Department waived contracting rules to allow Mississippi officials to move forward with their plans to hire contractors to rebuild the highway bridge and a similar bridge between Biloxi and Ocean Springs. Mineta explained that repairs couldn’t begin on either of the U.S. 90 bridges until much of the road was repaired between Gulfport and Biloxi so construction crews could get to the bridges. Work on the St. Louis Bay bridge is expected to begin as soon as early February.
Mineta 's remarks: http://www.dot.gov/affairs/minetasp012606.htm
Source: http://www.dot.gov/affairs/dot1306.htm

16. *January 26, Empire Information Services (NY)* — **New York's small airports to receive improvement funding.** New York State Department of Transportation (NYSDOT) Commissioner Thomas J. Madison Jr. on Thursday, January 26, announced $76.4 million in a new aviation improvement funding program that will help New York's small airports make infrastructure and aviation security improvements that will secure and modernize the State's public−use general aviation airports. The $76.4 million in Bond funds includes $30 million to improve aviation security, and will support improvements that include the installation of fencing, barriers, and lighting, and the construction of police substations for airports servicing aircraft weighing more than 12,500 pounds. To support regional economic development, $26 million of the funding will be used to support airports currently serving business aviation with existing runways of at least 3,000 feet in length. Projects must be shown to enhance existing business aviation service and demonstrate historical or projected business activity growth. The

$2.9 billion Bond Act is part of an overall five−year, $17.96 billion Department of Transportation capital program approved by the Governor and the Legislature last year, that will fund improvements to New York's multi−modal transportation system through 2010.
Source: http://www.eisinc.com/release/storiesh/NYSDOT.020.html

17. *January 25, GovExec* — **FAA accuses New York controllers of overtime abuse.** Federal Aviation Administration (FAA) officials claim that air traffic controllers in New York have abused sick leave, workers compensation, and overtime. Union representatives say the allegations are false. In a press conference Wednesday, January 25, FAA officials said controllers at the New York Terminal Radar Approach Control center, which handles air traffic from all three of New York's major airports, unnecessarily racked up more than $4 million in overtime pay in fiscal 2005. FAA took control over scheduling from the union this summer. As a result, agency officials said projected overtime costs for fiscal 2006 are less than $1 million. Jeffrey Clarke, the manager of the New York facility, said FAA discovered a significant amount of sick leave abuse at the facility. Clarke said controllers often would call in sick on days adjoining days off, such as the Monday after a weekend. Clarke said the agency asked some employees to bring in documentation for their sick leave and that the agency brought disciplinary actions on some employees.
Source: http://www.govexec.com/story_page.cfm?articleid=33239&dcn=to daysnews

18. *January 25, New York Times* — **MTA toughens terms of proposed transit contract.** The Metropolitan Transportation Authority (MTA) on Wednesday, January 25, proposed a contract considerably harsher than the one that the city's transit workers narrowly voted down on Friday, January 20, a move some labor experts said was designed to pressure union leaders to binding arbitration −− but could instead lead to new labor unrest. The authority's new offer keeps the provision that union members disliked most, a requirement that workers begin contributing 1.5 percent of their wages toward health−insurance premiums, and revives a proposal that had been taken off the table, that new workers contribute more to their pensions than current ones. It also includes provisions dropped early in the negotiations, like the expansion of one−person train operation. In addition, the authority's new offer eliminates a provision that delighted many workers: a pension refund that would give thousands of dollars to some 20,000 union members who made overpayments from 1994 to 2001. While some experts said the offer seemed to increase the possibility of another strike, others described it as a tactical move designed to show dissidents that the deal rejected last week was fair.
Source: http://www.nytimes.com/2006/01/25/nyregion/nyregionspecial3/ 25cnd−mta.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

19.

January 26, U.S. Department of Agriculture — **Funds for hurricane disaster assistance announced.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Thursday, January 26, announced $2.8 billion in aid to assist victims of the 2005 hurricane season. Agricultural producers will receive $1.2 billion through various programs and $1.6 billion will restore homes and rural communities. Johanns authorized the use of $250 million from Section 32 funds in October 2005 for crop disaster, livestock, tree and aquaculture assistance. These funds will be distributed by way of five new programs; the Tree Indemnity Program (TIP), the Hurricane Indemnity Program (HIP), the Livestock Indemnity Program (LIP), and the Feed Indemnity Program (FIP); and an Aquaculture Block Grant program. Producers in Alabama, Florida, Louisiana, Mississippi, North Carolina and Texas counties declared primary presidential or secretarial disaster areas in 2005 because of hurricanes are eligible to apply for assistance under the new programs. Prior to today's funding announcement, USDA has made available more than $1.7 billion to hurricane victims since September, bringing USDA's total hurricane aid to more than $4.5 billion.
Agricultural aid factsheet: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/01/0027.xml
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/01/0026.xml

20. *January 26, Palm Beach Post (FL)* — **Citrus greening spreads to trees in eleven Florida counties.** Citrus greening, an incurable citrus disease first detected in Florida in August, has now spread to 11 counties, a state entomologist said Wednesday, January 25. "Citrus greening is well−established in Florida, and we won't be able to get rid of it," said Susan Halbert, an entomologist with the Florida Department of Agriculture's Division of Plant Industry. The disease, which is fatal to citrus and is transmitted by an insect called the Asian citrus psyllid, has been identified in 408 residential properties and 10 commercial groves. The finds are in Palm Beach, Martin, St. Lucie, Monroe, Miami−Dade, Broward, Highlands, Collier, Hendry, DeSoto, and Sarasota counties. Surveyors are looking for more in the southwest part of the state, Halbert told growers attending the Indian River Citrus Seminar at the St. Lucie County Fairgrounds. University of Florida economist Ron Muraro said grapefruit growers who decide to stay in business and attempt to manage canker and greening can expect their costs to increase at least $200 to $300 an acre. But he thinks they can still make a profit.
Source: http://www.palmbeachpost.com/business/content/business/epaper/2006/01/26/a1d_greening_0126.html

[Return to top]

Food Sector

21. *January 26, Associated Press* — **Japan approves U.S. beef.** The 700 tons of U.S. beef distributed in Japan after the country eased its import ban last month is safe and can be eaten with no worries, Japan's agriculture minister said Thursday, January 26. Shoichi Nakagawa told parliament the meat was closely checked for banned material such as bone and brains when it entered the country. Japan halted imports again last week after it found banned spinal bones in a shipment of American veal. Nakagawa said about 1,500 tons of U.S. beef has entered Japan since the easing of a two−year−old ban on December 12, 2005. The ban was imposed in 2003 after the discovery of mad cow disease in an American herd. Of those 1,500 tons, more than

700 tons have already been distributed to supermarkets, restaurants and other outlets, but Nakagawa said that meat posed no health risk. Vice agriculture minister Mamoru Ishihara said Japan is considering limiting U.S. beef imports from about 10 facilities Japanese officials had inspected. Tokyo dispatched a team of inspectors to 11 facilities in five states −− Colorado, Kansas, Texas, Nebraska and California −− among dozens of exporters in December, days after announcing the easing of an import ban.
Source: http://www.chron.com/disp/story.mpl/ap/world/3614461.html

[Return to top]

Water Sector

22. *January 26, Philadelphia Inquirer (PA)* — **School's water being retested for E. coli.** Officials expect to know for sure Thursday, January 26, whether E. coli bacteria are in the water supply of Linden Elementary School in Doylestown, PA. Routine water tests detected the bacteria on Tuesday, January 24. No illness has been reported. Officials said they think the problem is with the test, not the water. While the test that came back Tuesday showed the presence of Escherichia coli, or coliform, it also showed good levels of chlorine. "Chlorine and coliform should not exist side by side, in theory. So we're at least cautiously hopeful that this is a testing anomaly," Doylestown Borough Manager John Davis said. For the second test, samples were also taken from the water distribution line. If there is a problem, that will help officials pinpoint it.
Source: http://www.philly.com/mld/inquirer/news/local/13714262.htm

23. *January 25, U.S. Environmental Protection Agency* — **New tool for determining cause of harm to rivers and streams.** The U.S. Environmental Protection Agency (EPA) has released a new Web−based tool, the Causal Analysis/Diagnosis Decision Information System (CADDIS), which simplifies determining the cause of contamination in impaired rivers, streams, and estuaries. An impaired body of water does not meet the state or federal water quality standards for one or more pollutants. More than a thousand U.S. water bodies have been identified as impaired, and in many cases, the cause is unknown. Before restorative or remedial actions can be taken, the cause of impairment must be determined. By helping to find the source of contamination, state and local organizations will be better able to implement the Clean Water Act. CADDIS provides a standardized and easily accessible system to help scientists find, use and share information to determine the causes of aquatic impairment. Causal analyses look at stressor−response relationships, meaning the effect of a specific substance or activity (stressor) on the environment. CADDIS was developed by EPA scientists through partnerships with EPA programs and regions, as well as states and tribes. The version of CADDIS released Wednesday, January 25, is the first of three.
CADDIS: http://www.epa.gov/caddis
Source: http://yosemite.epa.gov/opa/admpress.nsf/27166bca9a9490ee852570180055e350/9b73001491d0256885257101004984aa!OpenDocument

24. *January 06, Government Accountability Office* — **GAO−06−148: EPA Should Strengthen Ongoing Efforts To Ensure That Consumers Are Protected From Lead Contamination (Report).** Elevated lead levels in the District of Columbia’s tap water in 2003 prompted questions about how well consumers are protected nationwide. The Environmental Protection

Agency (EPA), states, and local water systems share responsibility for providing safe drinking water. Lead typically enters tap water as a result of the corrosion of lead in the water lines or household plumbing. EPA's lead rule establishes testing and treatment requirements. This report discusses (1) EPA's data on the rule's implementation; (2) what implementation of the rule suggests about the need for changes to the regulatory framework; and (3) the extent to which drinking water at schools and child care facilities is tested for lead. Among other things, the Government Accountability Office (GAO) recommends that EPA improve its data on key aspects of lead rule implementation, strengthen certain regulatory requirements and oversight, and assess the problem of lead in drinking water at schools and child care facilities. In commenting on a draft of this report, EPA generally agreed with our findings and recommendations.
Highlights: http://www.gao.gov/highlights/d06148high.pdf
Source: http://www.gao.gov/new.items/d06148.pdf

[Return to top]

Public Health Sector

25. *January 27, Associated Press* — **Indonesia reports new bird flu fatality.** An Indonesian market vendor died of the H5N1 strain of bird flu on Thursday, January 26, a hospital spokesperson said. The 22−year−old, who had a history of contact with dead poultry, died at Jakarta's Sulianti Saroso hospital for infectious diseases hospital, Ilham Patu said. Local test results released Wednesday, January 25, confirmed the man had bird flu. Blood and swab samples from the man have been sent to a World Health Organization approved laboratory in Hong Kong for confirmation. If they come back positive, Indonesia will raise its death toll to 15.
Source: http://www.thejakartapost.com/detaillatestnews.asp?fileid=20 060126172741&irec=2

26. *January 26, Agence France−Presse* — **Epidemic of crippling disease spreads in Indian Ocean island.** An epidemic of a crippling and incurable mosquito−borne disease has continued to spread throughout the Indian Ocean island of Reunion, with thousands of new cases reported. Only in the last week more than 5,600 new cases were reported, taking the total number of people infected by chikungunya to 22,167 on the French−ruled island since the beginning of the epidemic last March, said Gilles Brucker, director of a government health monitoring institute on Thursday, January 26. "We should expect that the number of cases will pass 30,000," Brucker said. "We should expect that the number of cases will pass 30,000," Brucker said. Chikungunya is Swahili for "that which bends up" and refers to the stooped posture of those afflicted by the disease for which there is no known vaccine or cure. Authorities on the volcanic island east of Madagascar, a French overseas department with a population of 760,000 and a popular holiday destination, have earmarked $720,000 to fight the outbreak, including special mosquito−eradication brigades.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://www.todayonline.com/articles/97607.asp

27. *January 26, Associated Press* — **Drug company to begin bird flu clinical trials.** Drug maker GlaxoSmithKline PLC hopes to start clinical trials in early April for its vaccine against the H5N1 bird flu strain, a company executive said Thursday, January 26. The United Kingdom

based company would test the vaccine with two different boosters and the first results should come about three months later, said David Stout, president of the company's pharmaceutical operations. Production is slated to start by year's end, he said on the sidelines of the World Economic Forum's annual meeting. GlaxoSmithKline has submitted a mock−up dossier to the European Agency for the Evaluation of Medicinal Products (EMEA) seeking an outline approval to market a vaccine against pandemic flu. The mock−up process requires companies to conduct clinical trials for safety and to establish the dosage and schedule for core compounds to obtain quick authorization for pandemic vaccines.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/n/a/2006/01/26/financial/f024900S05.DTL&type=health

28. *January 25, University of Wisconsin−Madison* — **Scientists unravel mystery of how flu viruses replicate.** University of Wisconsin−Madison researchers, led by virologist Yoshihiro Kawaoka, have found that influenza A viruses always organize the RNA fragments that make up the genetic contents of the virus in a circle of seven surrounding an eighth fragment. Like any other organism, an influenza virus's success in life is measured by its genetic track record, its ability to pass on genes from one generation to the next. But although much is known about the genes and inner workings of flu viruses, how the microbe organizes its genetic contents to seed future generations of viruses had remained an enduring mystery of biology. "We've found that the influenza virus has a specific mechanism that permits it to package its genetic materials" as it creates its infectious particles, says Yoshihiro Kawaoka, a veterinary medicine professor. "It was not really known whether the fragments were coming as a set," explains Kawaoka, whose team conducted the work using a long−studied influenza A virus. The fact that the virus requires a systematic −− as opposed to a random −− method of assembly opens the door to the development of new antiviral drugs and the harnessing of benign influenza viruses as gene vectors to optimize vaccine production, Kawaoka says.
Source: http://www.news.wisc.edu/12061.html

[Return to top]

Government Sector

29. *January 26, WTOC (GA)* — **Courthouse reopens after chemical evacuation.** The Chatham County Courthouse in Savannah, GA, is back open following Friday, January 20's evacuation and shutdown. The building was up and running, business as usual. On Friday, when chemical fumes from a cleaning agent known as xylene caused a few workers to get sick, the courthouse was shut down. No one was seriously injured, but Chatham County public health officials say emergency management did the right thing and avoided any major health issues. "We basically told them the levels people were exposed to, there was no long−term exposure, so there should be no long−term effects," said the health department's Chris Rustin. The chemical fumes were caused by a roofing contractor cleaning his equipment too close to an intake valve on the building's rooftop.
Source: http://www.wtoctv.com/Global/story.asp?S=4397353&nav=0qq6

[Return to top]

Emergency Services Sector

30. *January 26, Federal Computer Week* — **Federal Emergency Management Agency prepares for 2006 hurricane season.** With less than five months until the 2006 hurricane season starts, the Federal Emergency Management Agency (FEMA) is already preparing for this year's season, the agency's chief information officer (CIO) said Wednesday, January 25. "A lot of this won't get done before June 1," the first day of the season, CIO Barry West said at a gathering of the Industry Advisory Council/American Council for Technology in Falls Church, VA. To prepare for the 2006 hurricane season, FEMA has commissioned studies by Gartner Research and other organizations and is looking at industry best practices, West said. It is also helping bolster the Department of Homeland Security's new Preparedness Directorate, which is assuming FEMA's preparedness activities. The agency is implementing a six−part, agency−wide retooling effort that includes improving logistics, customer service and personnel, West said. Improvements for this year also include beefing up the National Emergency Management Information System (NEMIS), which tracks incident coordination efforts. FEMA intends to eventually upgrade NEMIS to handle three or four catastrophes at a time, West said. The agency could have the next−generation system in place for the 2007 hurricane season, he said.
Source: http://www.fcw.com/article92101−01−26−06−Web

31. *January 26, Associated Press* — **NTSB says all air ambulance crashes avoidable.** Federal safety investigators say 55 air ambulance crashes over the past three years, including a Colorado air ambulance crash last year, didn't have to happen. The National Transportation Safety Board (NTSB) made safety recommendations to the Federal Aviation Administration (FAA) Thursday, January 26. They suggest providing pilots with better training, night vision goggles, and crash avoidance systems. NTSB officials cite the Colorado crash as "the best examples of safety issues involved." On January Eleventh, 2005, a Colorado air ambulance crashed near Rawlins, WY, killing three people. But the FAA, which regulates aviation safety, says it believes voluntary cooperation with its current safety recommendations will improve air ambulance safety faster.
Source: http://www.9news.com/acm_news.aspx?OSGNAME=KUSA&IKOBJECTID=0806543e−0abe−421a−0155−7b7191900ca2&TEMPLATEID=0c76dce6−ac1f−02d8−0047−c589c01ca7bf

32. *January 25, Des Moines Register (IA)* — **Homeland Security will handle Iowa's Capitol evacuation.** Governor Tom Vilsack has directed Iowa's Homeland Security administrator to make sure all of the emergency evacuation plans at the state Capitol are coordinated in wake of concerns that disabled people could not get out of the building. "The governor gave that task to homeland security so they can actually coordinate all of the different agencies' evacuation plans," the governor's spokesperson Joseph Jones said Wednesday, January 25. "The general concern, obviously, is for the well being and safety of the people who visit the Capitol and who work in the Capitol. Homeland security will now have the function of actually making sure all of those agency plans are coordinated and actually enacted." In addition, Rep. Mark Kuhn (D−IA) told lawmakers Wednesday morning that he has asked the governor to set up a special task force of state leaders and experts to review the state's plans.
Source: http://www.desmoinesregister.com/apps/pbcs.dll/article?AID=/20060125/NEWS10/60125008/1001/RSS01

33. *January 25, Associated Press* — **Siren alert system to be tested Washington, DC, metro area.** Modernized sirens will be tested in Arlington and Alexandria, VA, and other local governments will be watching carefully. The Department of Homeland Security decided try the sirens after emergency managers determined that pager and e−mail alerts and other high−tech systems implemented since 9/11 still aren't enough to alert millions of area residents. In addition to a wail, the new sirens will broadcast information. Local residents will get vocal directions to move indoors, prepare to evacuate or turn on the radio or television for more details.
Source: http://www.wjla.com/news/stories/0106/297006.html

34. *January 25, El Paso Times (TX)* — **Texas city receives upgraded 911 call center.** This week, El Paso, TX, will move its 911 system into a new downtown building in what emergency communication staff describe as a major improvement. Call−takers for 911 and El Paso police and fire dispatchers began working Thursday, January 26, in their new building, which replaces the communications room at Police Headquarters. The building will also house El Paso's Emergency Operations Center, said Fire Department Communications Division Chief Chris Celaya. The new site allows for police and fire dispatchers to be in closer communication and includes phone and computer upgrades, including greater use of the highway cameras of the Texas Department of Transportation, officials said. The center could eventually house dispatchers for other agencies, such as police for Socorro, Horizon City and the El Paso Independent School District.
Source: http://www.borderlandnews.com/apps/pbcs.dll/article?AID=/20060125/NEWS/601250333

[Return to top]

Information Technology and Telecommunications Sector

35. *January 27, United Press International* — **AT&T to conduct disaster exercise.** AT&T will conduct its largest−ever network disaster recovery exercise in Dallas, TX, on Wednesday, February 8, the company said Wednesday, January 25. The telecommunications group said that self−contained equipment trucks will test and evaluate how well the company can support services in the event of a disaster. A total of 43 trailers will be used for the latest exercise in the Dallas−Fort Worth area. AT&T said it has invested over $300 million in its network disaster recovery program, which includes engineers and technicians across the country. The team has been activated 21 times since 1990, including responding to Hurricanes Katrina and Rita last year, the San Diego wildfires in 2003 and the September 11, 2001, attacks in New York City.
Source: http://www.physorg.com/news10220.html

36. *January 25, FrSIRT* — **Oracle PL/SQL Gateway exclusion list security bypass vulnerability.** A vulnerability has been identified in various Oracle products, which could be exploited by remote attackers to bypass security restrictions and gain unauthorized access to a vulnerable system. This is due to an input validation error in the PL/SQL Gateway component that does not properly handle malformed HTTP requests, which could be exploited by remote unauthenticated attackers to bypass the "PLSQLExclusion" list and gain access to "excluded" packages and procedures that will allow the compromise of the back end database server.

FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2006/0338

37. *January 25, FrSIRT* — **Cisco IOS TCLSH AAA command authorization bypass vulnerability.** A vulnerability has been identified in Cisco IOS, which could be exploited by malicious users to bypass security restrictions and obtain elevated privileges. This issue is due to an error in the Authentication, Authorization, and Accounting (AAA) command authorization feature that does not properly perform authorization checks on commands executed from the Tool Command Language (Tcl) exec shell, which could be exploited by authenticated users to bypass command authorization checks resulting in unauthorized privilege escalation. Solution: Apply fixes:
http://www.cisco.com/warp/public/707/cisco−response−20060125 −aaatcl.shtml
Source: http://www.frsirt.com/english/advisories/2006/0337

38. *January 25, FrSIRT* — **HP Oracle for Openview multiple remote and local vulnerabilities.** Multiple vulnerabilities were identified in Oracle for Openview (OfO). These flaws, initially reported in Oracle Critical Patch Update (January 2006), could be exploited by remote or local attackers to cause a denial of service, execute arbitrary commands, read and overwrite arbitrary files, disclose sensitive information, conduct SQL injection and cross site scripting attacks or bypass certain security restrictions. Solution: Apply Oracle Critical Patch Update (January 2006): http://www.oracle.com/technology/deploy/security/pdf/cpujan2 006.html
Source: http://www.frsirt.com/english/advisories/2006/0323

39. *January 25, FrSIRT* — **HP−UX local command execution and privilege escalation vulnerability.** A vulnerability has been identified in HP−UX, which may be exploited by malicious users to obtain elevated privileges. This issue is due to an unspecified error that could allow local attackers to execute arbitrary commands with elevated privileges.
Solution: HP−UX B.11.00 − Install PHCO_29249 or later
HP−UX B.11.04 − Install PHCO_32280 or later
HP−UX B.11.11 − Install PHCO_30402 or later
Source: http://www.frsirt.com/english/advisories/2006/0322

40. *January 25, Tech Web* — **Gartner bashes Oracle over security.** Oracle security practices are raising red flags, a Gartner analyst recently warned, and administrators should hunker down in protecting their database systems. Just five days after Oracle released a critical security update that patched 82 vulnerabilities, a Gartner researcher said in an online advisory that "Oracle can no longer be considered a bastion of security." Rich Mogull wrote, "The range and seriousness of the vulnerabilities patched in this update cause us great concern.... The database products alone include 37 vulnerabilities, many rated as easily exploitable and some potentially allowing remote database access. Oracle has not yet experienced a mass security exploit, but this does not mean that one will never occur." Mogull noted that Oracle administrators had avoided patching by relying on the database's strong security and the fact that the software was deployed deep within an enterprise's defenses. That no−patching procedure won't cut it now. To keep databases secure, Mogull recommended that companies shield all Oracle systems, patch known bugs −− "because incomplete information from Oracle will make shielding incomplete," he said in an aside −− and pressure Oracle to get on the security stick.
Source: http://www.techweb.com/wire/security/177103864;jsessionid=O4

0E1UZM0ACXCQSNDBGCKH0CJUMEKJVN

41. *January 25, CNET News* — **Skype could provide botnet controls.** Internet phone services such as Skype and Vonage could provide a means for cybercriminals to send spam and launch attacks that cripple Websites, experts have warned. Moreover, because many voice over Internet protocol (VoIP) applications use proprietary technology and encrypted data traffic that can't easily be monitored, the attackers will be able to go undetected. "VoIP applications could provide excellent cover for launching denial of service (DoS) attacks," the Communications Research Network said Wednesday, January 25. The Communications Research Network is a joint venture between Cambridge University and the Massachusetts Institute of Technology. The group urges VoIP providers to publish their routing specifications or switch to open standards. "These measures would...allow legitimate agencies to track criminal misuse of VoIP," Jon Crowcroft, a professor at Cambridge University in the UK, said in a statement. VoIP applications such as eBay's Skype and Vonage could give cybercriminals a better way of controlling their zombies and covering their tracks, the Communications Research Network said. "If the control traffic were to be obfuscated, then catching those responsible for DoS attacks would become much more difficult, perhaps even impossible," the group said in a statement.
Source: http://news.com.com/Skype+could+provide+botnet+controls/2100−7349_3−6031306.html?tag=cd.top

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 receiving reports of a new destructive email worm known as CME 24, which will actively disable anti−virus software on a host system and will also overwrite users' data files on the third of every month. This worm affects all recent versions of Microsoft Windows. CME 24 is also known as Nyxem.E, Blackmal.E, MyWife.d, BlackWorm, Tearec.A, Grew.a, and Kama Sutra.

This malcode spreads primarily by harvesting email addresses from files on the local machine and then emailing itself as an executable attachment. It uses subject lines such as "Photos", "*Hot Movie*", and "Miss Lebanon 2006" to entice the user into opening the attachment. As soon as the attachment is executed, the user's system is immediately infected. Infected hosts within a network enclave will also try to spread locally through network shares with weak passwords.

On the third of every month, CME 24 will over−write users' files on all accessible drives with the message "DATA Error [47 0f 94 93 F4 F5]". This will happen approximately 30 minutes after the user logins to the infected machine. The files affected by this variant will have the following file extensions: .doc, .xls, .mdb, .md3,

.ppt, .pps, .zip, .rar, .pdf, .psd, and .dmp.

The infected host will also access a website containing a counter. The web counter shows how many machines have been infected, although it is expected that an infected machine may access that website on multiple occasions, thus inflating the number. The web counter has shown consistent growth with over 500,000 infections on Saturday and is now currently showing over 700,000 infections. FBI agents have received log data that resided on the web server, and is sharing the bulk data with US−CERT for analysis.

As CME 24 disables anti−virus systems, it leaves infected computers wide open to attack by other malware variants. All major anti−virus companies are offering signature files that should prevent infection. In addition, major anti−virus vendors are offering tools and instructions for removing this variant from their systems.

US−CERT has not received any reports of infections within the Federal space. Currently, US−CERT is coordinating the analysis of log file data that could be an indicator of infected systems, and will be distributing notifications to affected parties.

Nyxem Mass−mailing Worm US−CERT is aware of a new mass mailing worm known as Nyxem (CME−24). This worm relies on social engineering to propagate. Specifically, the user must click on a link or open an attached file.The Nyxem worm targets Windows systems that hide file extensions for known file types (this is the default setting for Windows XP and possibly other versions). The worm's icon makes it appear to be a WinZip file. As a result, the user may unknowingly execute the worm. For more information please review: http://cme.mitre.org/data/list.html#24

US−CERT strongly encourages users not to follow unknown links, even if sent by a known and trusted source. Users may also wish to visit the US−CERT Computer Virus Resources for general virus protection information at URL: http://www.us−cert.gov/other_sources/viruses.html

Current Port Attacks

Top 10 Target Ports	6881 (bittorrent), 1026 (win−rpc), 445 (microsoft−ds), 25 (smtp), 65535 (Adoreworm), 135 (epmap), 139 (netbios−ssn), 80 (www), 6884 (−−−), 32768 (HackersParadise) 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

Nothing to report.

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact DHS

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

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

Department of Homeland Security Disclaimer