Department of Homeland Security Daily Open Source Infrastructure Report for 29 January 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

- According to the EE Times, cybersecurity standards to protect the nation's power grid from disruption were approved by the Federal Electric Regulatory Commission (FERC) earlier this month. The new standards will require energy companies to identify and document risks and vulnerabilities and establish controls to secure critical assets from sabotage. (See item 3)
- CNN reports that a covert tester for the Transportation Security Administration managed to enter the Tampa International airport with a bomb strapped to his back, despite having setting off the scanner and having been patted down. TSA officials say this test demonstrates the type of systemic vulnerability that the agency is working to expose and address. (See item 10)

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 27, Financial Times* – (International) **Investors shift bets to oil slide.** Investors are shifting their bets towards oil prices weakening in the near future as the slowdown in U.S. economic activity dampens energy demand growth, traders in London and New York said. The reversal in investor mood is reflected in the buying of options contracts that will be only profitable if prices fall by mid-year below $80 a barrel. Crude oil has

been trading in a range of $80-$100 a barrel since mid-October. An energy trader at the investment bank Macquarie said that last week investors had bought large volumes of put options, particularly for the second half of the year. “Hedge funds are losing heart on the bullishness of the oil market,” he said. Investors are beginning to unwind some of the positions they built as bets that oil prices will this year trade above $100 -- and even as high as $200 a barrel. The shift in sentiment is subtle, however, and investors continue to anticipate that prices in 2008 will be higher on average than last year.
Source: http://www.ft.com/cms/s/0/d42c4e06-cd2c-11dc-9b2b-000077b07658,s01=1.html

2. *January 27, Associated Press* – (National) **Official: U.S. mine violations ignored.** The Mine Safety and Health Administration (MSHA), the federal agency that regulates the nation’s mining industry, says it has failed to issue penalties for hundreds of citations issued since 2000, and the problem could extend as far back as 1995. Preliminary data showed that penalties had not been assessed against about 4,000 citations issued by the agency between January 2000 and July 2006, the Charleston Sunday Gazette-Mail reported. The MSHA director told the newspaper that the review also showed that penalties had never been assessed for a few hundred citations issued in 1996. In a speech given to West Virginia coal operators earlier this month, the director told mine operators that MSHA had improved its inspection and assessment process over the past year. He said the number of assessments against coal operators had increased from $20.2 million in 2006 to $40.4 million in 2007.
Source: http://www.usatoday.com/news/nation/2008-01-27-mines-penalities_N.htm?csp=15

3. *January 25, EE Times* – (National) **New cybersecurity specs target power grid.** Cybersecurity standards to protect the nation’s power grid from disruption were approved by the Federal Electric Regulatory Commission (FERC) earlier this month. The new standards will require energy companies to identify and document risks and vulnerabilities and establish controls to secure critical assets from sabotage. They also mandate that energy companies report “security incidents” and set up emergency recovery plans, according to the North American Electric Reliability Corp., which ensures reliability of the bulk power system. The new standards, which require compliance by 2010, will become mandatory in March. Energy industry watchers approved the move. “Tests have shown Scada [Supervisory Control and Data Acquisition] hacking can work,” said the chief executive officer of TECSys Development Inc. “Our government, the CIA, believes that one of our biggest threats is state-funded agencies or hackers working toward getting access to our nation’s critical infrastructure,” he added.
Source: http://www.eetimes.com/rss/showArticle.jhtml?articleID=205918880&pgno=1

[Return to top]

Chemical Industry Sector

4. *January 26, Salt Lake Tribune* – (Utah) **Fire crews clean up industrial chemical spill; no one hurt.** On Saturday, a chemical spill at the Thatcher Co. in Salt Lake City left fire crews cleaning up about 550 gallons of a chemical mixture. The spill sent an orange-

yellow cloud from the company's scrubber system, he said. A mixture of calcium nitrate, calcium nitrite, and an unidentified third product spilled into the building. A deputy fire chief called the mixture "extremely acidic" and said employees used caustic soda to neutralize the spill before pumping it into a holding tank. "They accidentally mixed two chemicals and that's what caused the reaction," he said. He said the company appears to be in compliance with all safety regulations and the incident has been ruled an accident. The official added that liquid from the spill was kept within the building, but some "gaseous product" was emitted from the scrubbers. No injuries were reported.
Source: http://www.sltrib.com//ci_8083731

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *January 28, TVNZ News* – (South Carolina) **Nuclear workers show higher cancer risks.** Workers at the Savannah River nuclear facility in South Carolina have suffered higher-than-average rates of certain cancers, a study shows -- suggesting that on-the-job exposures are to blame. Researchers at a university found that while death rates from many causes were lower than national rates, workers had higher-than-expected rates of death from certain cancers. Among men, leukemia and cancer of the pleura caused an abnormally high number of deaths, while female workers had elevated rates of kidney and skin cancers. The study included 18,883 employees who were hired prior to 1987 and worked at the nuclear facility for at least three months. "It is plausible," the researchers wrote, "that occupational hazards, including asbestos and ionizing radiation, contribute to these excesses."
Source: http://tvnz.co.nz/view/page/1318360/1560925

6. *January 27, Valley News Dispatch* – (Pennsylvania) **EPA to advise on cleanup of nuke waste.** The federal Environmental Protection Agency (EPA) will sit in on a planning meeting next month on the cleanup of a nuclear waste dump in Armstrong County, Pennsylvania. Known as the Shallow Land Disposal Area (SLDA), the site along Route 66 in Parks was established in the late 1950s as a dump for nuclear and chemical waste. Dumping ceased at the site in 1970, according to government agencies. The SLDA contains 50,000 tons of radioactive-contaminated materials and a host of dangerous chemicals, including benzene, vinyl chloride, and trichloroethylene. The U.S. Army Corps of Engineers is leading a $45 million cleanup effort, but is authorized by Congress to handle only radiological contamination. The state has jurisdiction over chemical remediation. The Corps' cleanup is scheduled to begin this summer and continue until 2013. Activists are pressing the state Department of Environmental Protection to involve the EPA because of concerns about chemical remediation and cleanup standards. The EPA has experts in environmental cleanup with more stringent standards than the Army Corps, an activist said. "EPA does not have a regulatory role for cleaning up the radiological waste," an EPA spokesman said.
Source:
http://www.pittsburghlive.com/x/pittsburghtrib/news/cityregion/s_549514.html?source=rss&feed=1

[Return to top]

Defense Industrial Base Sector

7. *January 27, Associated Press* – (National; International) **Dead spy satellite could hit Earth within a month, officials say.** A large U.S. spy satellite has lost power and could hit the Earth in late February or early March, government officials said Saturday. The satellite, which can no longer be controlled, could contain hazardous materials, and it is unknown where on the planet it might come down, they said. It was not clear how long ago the satellite lost power, or under what circumstances. "Appropriate government agencies are monitoring the situation," said a spokesman for the National Security Council. "Numerous satellites over the years have come out of orbit and fallen harmlessly. We are looking at potential options to mitigate any possible damage this satellite may cause," he said. He would not comment on whether it is possible for the satellite to perhaps be shot down by a missile. A senior government official said that lawmakers and other nations are being kept apprised of the situation. Such an uncontrolled re-entry could risk exposure of U.S. secrets, said a defense and intelligence expert. He estimated that the spacecraft weighs about 20,000 pounds and is the size of a small bus. He said the satellite would create 10 times less debris than the Columbia space shuttle crash in 2003.
   Source: http://www.foxnews.com/story/0,2933,325829,00.html

[Return to top]

Banking and Finance Sector

8. *January 28, Computerworld* – (National) **Data breach affects 650k customers of 230 retailers.** An unencrypted backup tape containing credit card information on customers of 230 U.S. retailers was discovered missing in October, the company responsible for the data confirmed earlier this month. GE Money USA, which manages in-store credit programs for retailers, said the tape held credit card information on about 650,000 customers. The General Electric Co. subsidiary said the tape contained the Social Security numbers of 150,000 of those customers. A GE Money spokesman confirmed that J.C. Penney Co. was affected by the breach, but he declined to identify other retailers whose data was on the tape. The spokesman said the tape was found to be missing from an Iron Mountain Inc. facility in October. An Iron Mountain spokesman said that the firm regretted the incident, but he added that there is "zero evidence that the media has been obtained by unauthorized people and misused in any way." GE Money has set up a toll-free number for customers and is offering free credit-monitoring services to those affected.
   Source:
   http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=storage_security&articleId=311724&taxonomyId=153

9. *January 28, KMBC 9 Kansas City* – (National) **FBI warns of tax-rebate scam.** If lawmakers pass an economic-stimulus package, it could mean people will receive a check in the mail. Some families could receive thousands of dollars. But the FBI is

warning that some people are using the story to steal. Scammers, pretending to be IRS agents, are calling unsuspecting people, asking for Social Security numbers and other personal information so a refund check can be sent. An FBI special agent said they have four reports so far in the Kansas City area. He said scam artists are doing what is called phishing -- fishing for unsuspecting victims. The tax-rebate plan has not even been approved by Congress yet, and the IRS will never ask for personal information on the phone or in an e-mail.
Source: http://www.kmbc.com/news/15152423/detail.html

[Return to top]

Transportation Sector

10. *January 28, CNN* – (Florida) **TSA tester slips mock bomb past airport security.** A covert tester for the Transportation Security Administration has been probing airport weaknesses for five years, beginning with big mock bombs before switching to ever-smaller devices as the TSA adapts to evolving terrorist threats. He went through the metal detector portal at Tampa International airport in Florida, and the detector alarm went off – as he expected it to – not because of the nonmetallic device strapped to his back, but due to his metal knee. A screener "wanded" him with a hand-held metal detector, and it beeped as it passed his metal knee, his necklace, and the rivets on his blue jeans. The screener then patted him down, running latex-gloved hands over his legs, arms, and torso. He patted down his back, including the lower part where the device was concealed. But the tester explained away the back support. He told the screener that he had a bum back in addition to having a metal knee. With the pat down over, the screener released him. He picked up his belongings and walked freely into the airport, the fake bomb still fastened to his back. TSA officials say the Tampa test demonstrates the type of systemic vulnerability that the agency is working to expose and address. Screeners have cultural sensitivities toward travelers' handicaps, and they are sometimes hesitant to perform intrusive searches, officials said. Terrorists could exploit that reluctance, they said. After leaving the screening checkpoint, the tester returned with other members of his red team and informed the screener he has failed a test. A fake bomb has just entered their airport. Regardless of their reactions, screeners who fail to detect contraband are "pulled off the line" and retrained before being allowed back. The TSA says techniques such as the one used in Tampa are known to terrorists and openly discussed on known terror Web sites.
Source: http://www.cnn.com/2008/US/01/28/tsa.bombtest/

11. *January 28, Associated Press* – (Washington) **Southwest Airlines plane skids off snow-covered runway in Washington.** A Southwest Airlines plane with 118 passengers on board skidded off a snow-covered taxiway Sunday afternoon after safely landing at Spokane International Airport in Washington, the airline said. The pilot was slowly taxiing to the gate when the front wheels of the plane slid off the taxiway around 1:40 p.m., said a spokeswoman for the Dallas-based carrier. The airport shut down operations until crews could move the Boeing 737, which was obstructing a taxiway. The plane was moved at about 4:30 p.m., and flights resumed shortly after 5 p.m., the airport said. The plane originated in Albuquerque, New Mexico, then flew to San Diego,

Sacramento, California, and Portland, Oregon, before heading to Spokane, said the spokeswoman. No one was injured.
Source: http://www.foxnews.com/story/0,2933,325895,00.html

12. *January 28, Associated Press* – (California) **Storms close California roads.** Several major roadways across the state were closed early Monday after the latest in a week's worth of storms, and experts warned that the risk of mudslides has not eased even as wet weather begins moving out of the region. Snow forced the closure of the main artery between Sacramento, California, and Reno, Nevada, the California Department of Transportation said Sunday night. Eastbound Interstate 80 was closed about 50 miles northeast of Sacramento, and westbound traffic was being held at the Nevada state line. Officials also closed a nearly 130-mile stretch of Interstate 395, from just north of Bishop to the Nevada line. Experts say hillsides in Los Angeles, Orange, and San Diego counties, charred by last year's wildfires, remain at risk for landslides. Near San Diego, mud and minor rockslides prompted California Highway Patrol officials to shut Route 78 through a burn area between Ramona and Escondido.
Source:
http://ap.google.com/article/ALeqM5gIqj9If0XazeSoYijSrM92ANAHVQD8UETL000

13. *January 27, Sunday Times* – (National) **Ten-finger scan to get into USA.** Security screening for arriving passengers has been stepped up at American airports, but the Sunday Times has learnt of worrying flaws in new fingerprint-scanning technology. Non-U.S. residents have had two fingers scanned on entry since 2004, but the Department of Homeland Security believes the 10-finger standard will allow easier identification of undesirables, based on full or partial prints left at the scene of a crime or collected from terrorist safe houses or battlefields. Described by Identix, their manufacturer as "slap and roll" technology, the scanners require four scans to capture a full set of prints. However, the system has caused problems in the past. In 2003, a Californian filed a lawsuit after he was stopped by police for a traffic violation and fingerprinted using the same scanner. His prints were incorrectly matched with a convicted felon, and he served 43 days in prison. Another man brought a lawsuit against Identix in 2004 after his prints were wrongly assigned to a convicted murderer. The case was dismissed after the judge ruled that human error, and not the scanner, had caused the mix-up, but human-rights groups say overdependence on technology will continue to put travelers at risk. Last July, a U.S. government report found that "systems supporting the US-VISIT program have significant information security control weaknesses," but the homeland security chief is an enthusiast. "Moving to 10 fingerprints is completely consistent with, and in fact enhances, our ability to protect," he said.
Source: http://travel.timesonline.co.uk/tol/life_and_style/travel/article3250494.ece

14. *January 26, Seattle Times* – (Idaho) **Man seeking shoe shine trips security worries at Boise airport.** Authorities say a California man bypassed a security checkpoint at Boise Airport in his quest for a shoe shine, a breach that led to an 80-minute shutdown of the terminal, delayed four flights and required re-screening of at least 400 passengers. A Transportation Safety Administration spokesman said the man left a secure area of the terminal and was seen by passengers using an exit door to enter the concourse. After

confirming what had happened by checking a video camera, police and airport security began the search and shutdown of the airport. During the search, a shoe shine employee shared information on a possible identity, Boise police said. Security then obtained the man's cell phone number and called him and asked him to return to the airport. Police said the man was cooperative, acknowledged breaching security to get his shoes shined and was released. He was cited for failure to be screened before entering a secure area, a misdemeanor, the Boise Police Department said in a statement. The violation is punishable by a maximum six months in jail. He also could face maximum fines of $3,000 from the U.S. Department of Homeland Security.
Source:
http://seattletimes.nwsource.com/html/localnews/2004146569_apidairportsecuritybreach1stldwritethru26.html?syndication=rss

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture and Food Sector

15. *January 26, Associated Press* – (National; Nebraska) **USDA lab focuses on deadly E. Coli.** Scientists at the Roman L. Hruska U.S. Meat Animal Research Center in Nebraska are conducting research into the increasing number of beef recalls and rising levels of E. coli contamination. The lab has its own feedlot and a herd of about 6,500 cows that are used for genetic research. In 2007, more than 30 million pounds of ground beef were pulled off the market in 20 recalls because of possible E. coli contamination. That included the second-largest recall in U.S. history, which put Topps Meat Co. out of business. One of the lab's current projects will test whether feeding cattle distiller's grain – a byproduct of making the gasoline additive ethanol – has any effect on the level of E. coli and the quality of meat produced. The Nebraska Corn Board suggested the distiller's grain research last spring, and the lab agreed because more and more feedlots are using the ethanol byproduct. The research involves 600 cattle. Half are being fed a traditional grain feed and half are being fed distiller's grain. The research will wrap up in June after the cattle have been sold for slaughter and samples of their carcasses have been collected.
Source:
http://news.yahoo.com/s/ap/20080126/ap_on_sc/e__coli_detectives;_ylt=Aum_X4hceQfhfU7De9ztpxKs0NUE

[Return to top]

Water Sector

16. *January 28, Post-Tribune* – (Indiana) **Toxic water cleanup lags.** Environmentalists say

the Indiana Department of Environmental Management has focused on completing studies of rivers and streams whose levels of E. coli bacteria are too high. Meanwhile, studies of Northwest Indiana waters that are impaired for mercury, polychlorinated biphenyls, and other toxic pollutants are left unfinished, which means clean-up plans are delayed. The executive director of Save the Dunes Council said the waters polluted by bioaccumulating chemicals should have priority. "We drain into the largest collection of freshwater in this country. I understand you need to have TMDL (studies) on waters flowing out of this state. But these are waters that drain into people's drinking water and have a retention of 99 years," he said. The Clean Water Act requires IDEM to identify waters that do not meet water quality standards and prioritize the waters based on the severity of the pollution. The states are then supposed to complete so-called total maximum daily load (TMDL) studies of where the pollution comes from so the problem can be addressed. One way to do that is to limit how much of the pollutant various facilities can discharge. An IDEM spokeswoman rejected the executive director's criticism, saying Indiana does better than many other states.
Source: http://www.post-trib.com/news/762263,impaired.article

[Return to top]

Public Health and Healthcare Sector

17. *January 28, BBC* – (International) **India bird flu disease 'alarming.'** The bird flu epidemic has spread further in the Indian state of West Bengal, with 13 of the state's 19 districts affected, officials say. An outbreak has been reported from Budge Budge, a suburb of the capital, Calcutta. A minister said that the situation was "alarming" Officials say more than 2.5 million birds would be culled. Though no human cases have been reported, health experts have warned that the outbreak could get out of control. What is worrisome is that the flu is affecting the populous state capital, Calcutta. On Thursday, tests on dead birds from Balagarh, less than a two-hour drive from Calcutta, tested positive for the disease. Tens of thousands of rural families, for whom poultry is a major source of income – if not the only one – have been ruined, and many more may face the same fate as the epidemic seems to be spreading. The economic consequences of this has lead to villagers resisting culling of their backyard poultry in many districts. Experts say this may explain the spread of the virus. The problem is made worse because many poor and illiterate farmers are sometimes misinformed about basic hygiene. Federal officials have warned that if the pace of culling does not pick up fast, the airborne virus may spread to the remaining districts and finally hit Calcutta.
Source: http://news.bbc.co.uk/2/hi/south_asia/7212486.stm

18. *January 28, Nursing Spectrum* – (National) **MRSA test approved.** The first rapid blood test for the drug-resistant staph bacterium methicillin-resistant staphylococcus aureus (MRSA) won U.S. Food and Drug Administration (FDA) approval for marketing. The BD GeneOhm StaphSR Assay uses molecular methods to identify whether a blood sample contains genetic material from the potentially fatal MRSA bacterium or a more-common, less-dangerous staph bacterium that still can be treated with methicillin. "Rather than waiting more than two days for test results, healthcare personnel will be able to identify the source of a staph infection in only two hours, allowing for more

effective diagnosis and treatment," said the director of the FDA's Center for Devices and Radiological Health in a statement.
Source:
http://include.nurse.com/apps/pbcs.dll/article?AID=/20080128/NATIONAL02/80125040/-1/frontpage

19. *January 27, Philadelphia Inquirer* – (Pennsylvania) **Norovirus sickens about 100 students at Villanova.** About 100 Villanova University students were stricken with symptoms of acute gastroenteritis most likely related to a norovirus, officials said Saturday. Fourteen were referred to emergency rooms for treatment of dehydration and then released. The students live both on and off campus and did not have a common food source, officials said. Yesterday, officials said the number of new cases with virus-related symptoms had decreased significantly. According to the federal Centers for Disease Control and Prevention, norovirus is highly contagious. It can be contracted through contaminated food or liquids or by touching a contaminated surface and then putting unwashed hands into the mouth.
Source:
http://www.philly.com/inquirer/local/philadelphia/20080127_Norovirus_sickens_about_100_students_at_Villanova.html

Government Facilities Sector

20. *January 28, WRC 4 Washington, DC* – (District of Columbia) **White House north lawn evacuated.** The north lawn of the White House has been evacuated while a suspicious package is investigated. The Secret Service evacuated the north lawn and stopped foot traffic on Pennsylvania Avenue in the area after a man was arrested for apparently making a threat against President George W. Bush, authorities said. The man was arrested along the fence line, the Secret Service reported. He had a duffle bag with him that was deemed suspicious.
Source: http://www.nbc4.com/news/15156192/detail.html?rss=dc&psp=news

21. *January 28, WRC 4 Washington, DC* – (District of Columbia) **Gas leak leads to evacuation of Senate day care.** A gas leak in the District of Columbia caused evacuations on Monday. In Washington, DC, the Senate day care center on Capitol Hill was evacuated at about 9:30 a.m. because of a gas leak. The Senate page dorm buildings were also evacuated as a precaution. There were no reported injuries. People were allowed to return to the buildings at about 10:30 a.m.
Source: http://www.nbc4.com/news/15153141/detail.html

22. *January 27, Associated Press* – (Texas) **Major military base realignment means boom for San Antonio.** The fifth and latest round of the base closure and realignment process, ordered by Congress in 2005, will move nearly 5,000 extra military jobs to San Antonio, a community with an already large Defense Department presence. The moves, to be completed by 2011, will include an estimated $2.1 billion in renovation and construction at Army and Air Force installations in the Alamo City. The realignment

will most affect Fort Sam Houston, a 131-year old garrison in the middle of San Antonio. The post, which already is the headquarters for the Army's medical command, will become the center for all Defense Department medical training and research.
Source:
http://www.statesman.com/news/content/news/stories/local/01/27/0127brac.html

[Return to top]

Emergency Services Sector

23. *January 28, Cumberland Times News* – (Maryland; Virginia; West Virginia) **Statewide communications system won't take away Hampshire fire unit's ability to talk with Virginia companies.** Some Capon Bridge, West Virginia, volunteer firefighters are concerned that the county's move toward a statewide emergency communications system may leave them unable to talk to companies in Virginia, on whom they rely for assistance during emergencies. Capon Bridge is only one mile from the Virginia state line and Gore County, Virginia, responds to many of their calls. The County Office of Emergency Services Director attended a Tuesday county commission meeting to explain that the company will not lose its ability to communicate with Virginia responders. He said the new equipment will have a channel the users can change to talk to Virginia providers, and they can also keep their high-band radios operational until 2013. "That's when we will have to be using all low-band frequencies," he said, adding that even then only their oldest high-band radios, those purchased before 1994, will have to be replaced.
Source: http://www.times-news.com/local/local_story_028115312.html

24. *January 28, Jackson County Chronicle* – (Wisconsin) **Proposed EMS upgrade means more services offered.** The Black River Falls Public Safety Committee learned of plans for a service upgrade for the Black River Falls Emergency Medical Services. The completion of a feasibility study and a public meeting are two of eight steps to be completed as part of a service upgrade, according to the State of Wisconsin Department of Health and Family Services. If a service upgrade were approved, EMS personnel would be required to complete a program of training based on the Wisconsin EMT-Intermediate Technician Curriculum. As a result of a service upgrade, EMS personnel would be authorized to provide more services to patients who utilize emergency medical services. The Black River Falls public safety committee unanimously approved providing a letter of support in favor of the service upgrade. The service upgrade request will now be forwarded to the Black River Falls City Council.
Source: http://www.jacksoncountychronicle.com/articles/2008/01/28/news/04ems.txt

25. *January 28, Herald-Star* – (International) **TEMS gets Homeland Security grant.** The TEMS Joint Ambulance District, which serves Toronto and part of Ohio, has received a grant from the U.S. Department of Homeland Security for a communications device to make it easier for the agency to communicate with other safety forces and agencies. The grant from the federal agency's Commercial Equipment Direct Assistance Program will enable the medical emergency agency to acquire the communications device as well as training on how to use it, according to TEMS' chief of operations. "The device is

portable, and you can take it anywhere," he said. "We could use it for everything from a small incident to a large-scale event. We'll get the device after we get the training on how to use it."
Source: http://www.hsconnect.com/news/articles.asp?articleID=21552

[Return to top]

Information Technology

26. *January 28, Computerworld* – (National) **Most malware is launched from legit web sites.** The majority of Web sites serving up attack code are legitimate domains that have been hacked by criminals, according to security research firm Websense Inc. In a report released last week, San Diego-based Websense said that credible sites accounted for 51 percent of those classified as malicious. Hacking legitimate sites so that they can sling malware gives attackers distinct advantages, said the vice president of security research at Websense. He noted that hackers have been aided by "the growth in social networking sites and blogs, where security is just not one of the ingredients. Hackers are saying, 'It's easier to put our malware on these sites than to build our own.'"
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=cybercrime_and_hacking&articleId=311713&taxonomyId=82&intsrc=kc_top

27. *January 27, Computerworld* – (National) **Windows Home Server vulnerable to critical bug, too.** For the second time in three days, Microsoft Corp. added another product to the list of those vulnerable to a critical bug patched nearly three weeks ago. Windows Home Server, the company's newest operating system, is also at risk to the vulnerabilities spelled out by the MS08-001 security bulletin, according to a Friday update. The advisory, first issued on January 8 -- and then fingered by researchers as the month's most pressing -- was revised Wednesday, when Microsoft announced that Windows Small Business Server was at risk. Neither Windows Home Server nor Small Business Server had been among the versions mentioned in the original bulletin. The initial bulletin had pegged the threat to Windows Server 2003 as "important," the second highest rating in Microsoft's four-step scoring system. But it was later rated as "critical" for Windows Home Server and Small Business Server. According to Microsoft, the vulnerability can be exploited by sending malicious data packets to unsuspecting users, who could find their PCs infected with malware or under the control of others. Within 10 days of Microsoft posting its first patches, researchers had produced proof-of-concept exploits, claiming that the company had overestimated the difficulty in crafting attack code. Windows Home Server owners have been offered the patch via the software's update mechanism, Microsoft said in the revised bulletin. Microsoft did not say why it had not identified Windows Home Server or Small Business Server as vulnerable and requiring repair when it first issued updates earlier this month.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9059378&intsrc=hm_list

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

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

[Return to top]

Communications Sector

28. *January 28, Wall Street Journal* – (National) **FCC pushes to overhaul subsidy program for rural phones.** Alarmed at the growth of a multibillion-dollar federal phone-subsidy program, regulators are beginning an effort to curb costs and prevent consumers from paying more in fees. As soon as Monday, the Federal Communications Commission is expected to open for public comment several proposals to revamp the Universal Service Fund, which subsidizes phone services for low-income and rural customers. The program's budget ballooned to about $7 billion last year from $5.2 billion in 2002 as more companies sought to tap the federal revenue stream -- a transfer of money collected from consumers through surcharges on phone bills. The charge is usually found on a phone bill itemized as a "federal universal service charge." One proposed change calls for using a reverse-auction system to pick which phone companies receive multimillion-dollar payments for providing phone service in rural areas. A separate plan would lower the amount of money wireless companies receive to offer service in rural areas. For the first time, the FCC also will look into whether money should be set aside to subsidize broadband Internet lines.
    Source:
    http://online.wsj.com/article/SB120148455929220793.html?mod=googlenews_wsj

29. *January 28, Associated Press* – (National) **Cell phone can read documents for blind.** A National Federation of the Blind (NFB) cell phone that incorporates text-to-speech software will soon be commercially available. The software reads images photographed by the phone, allowing blind users to decipher anything that is photographed, whether it is a restaurant menu, a phone book or a fax. The phone can scan limited amounts of text, read it aloud, and even translate from other languages. Future versions of the device will recognize faces, identify rooms, and translate text from other languages for the blind and the sighted. The inventor plans to begin marketing the cell phone in February through K-NFB Reading Technology. The software will cost $1,595 and the cell phone is expected to cost about $500.
    Source:
    http://news.yahoo.com/s/ap/20080128/ap_on_hi_te/blind_cell_phone;_ylt=AiCVvT3htQfQSe9eM16oO5H67rEF

[Return to top]

Commercial Facilities Sector

30. *January 25, Washington Times* – (Arizona) **Super Bowl deemed a target in federal threat assessment.** The upcoming Super Bowl game will be a desirable target for

terrorists, according to a threat assessment by federal security officials, which outlines several scenarios of possible attacks and security precautions for the February 3 event. Domestic and international terrorists have targeted major sporting events in the past, including the 1972 Munich and 1996 Atlanta Olympic Games, said the assessment compiled by the FBI and Homeland Security Department. The assessment, dated January 14 and obtained by the Washington Times, reminds law-enforcement officers of past incidents near stadiums, including an October 2005 incident in which a University of Oklahoma student blew himself up near the Gaylord Family-Oklahoma Memorial Stadium. It also warns that many thefts of government and law-enforcement property that could be used to facilitate entry have been reported in Arizona. Since October 2004, the Arizona Counter Terrorism Information Center has received more than 300 reports of thefts from fire, first responder, military, and police personnel including from those in the Phoenix area, where the game will be played.
Source: http://www.washingtontimes.com/apps/pbcs.dll/article?AID=/20080125/NATION/886850805/-1/RSS_FP

[Return to top]

National Monuments & Icons Sector

31. *January 26, Daily Record* – (Colorado) **Hiker reports damage to Pike monument.** A monument erected in 1946 was reported vandalized Thursday after a hiker noticed it was damaged. He said he found the plaque bent, but still attached to the stone. “It looks like someone tried to take it out with a crowbar,” he said. “It’s all bent. I don’t know if it can be repaired or if they will have to make a new one.” The monument honors Captain Zebulon Pike and his men, who explored the area in 1806, and the Santa Fe and Rio Grande employees, who fought in the Royal Gorge railroad war of 1878.
Source: http://www.canoncitydailyrecord.com/default.aspx?tabid=71&pDesc=2407,1,1

32. *January 26, Los Angeles Times* – (Alaska) **New fight looms on Tongass.** More than 3 million acres of wilderness in Alaska’s Tongass National Forest would be open to logging and road building under a management plan released Friday by the U.S. Forest Service. Of this acreage, about 2.4 million are in roadless areas, and about 663,000 acres are considered to have trees valuable for timber production. Local political officials hailed the plan as a reasonable way to maintain the area’s logging economy. But environmentalists portrayed it as the latest in a series of attempts by the current administration to dismantle protections of roadless areas and open them to logging before the current president leaves office. The plan adds 39,000 acres to old-growth reserves that are off-limits to logging and protects 47,000 acres of “karst” lands, which are limestone formations considered vulnerable to development. The Forest Service also plans to consult with native Alaskan tribes to protect and maintain sacred sites.
Source: http://www.thenewstribune.com/news/nationworld/story/265271.html

[Return to top]

Dams Sector

33. *January 27, Times-Reporter* – (Ohio) **Buildup: Anchors to improve Dover Dam strength.** A project manager for the Huntington District of the U.S. Army Corps of Engineers led a tour this week into the Dover Dam's gallery – a tunnel running through its center – to check the progress of a project to anchor the structure into the bedrock below with 17 three-inch-wide metal bars. The project is a stop-gap measure to temporarily address what the Corps calls a "hydrologic deficiency" – meaning the dam would not stand up to the level of flooding the Corps would like it to, partly because of faulting in the limestone and shale on which it rests. Work began December 17, and the contractor has 150 calendar days to finish the project.
Source: http://www.timesreporter.com/index.php?ID=78641

34. *January 26, Telegraph* – (New Hampshire) **Dams not to blame for April floods.** Last April's severe flooding along New Hampshire's Souhegan River was caused by heavy rainfall and melting snow pouring off frozen, saturated ground rather than by water released from dams in Wilton and Greenville, according to a preliminary study by the state. "The dams in the Souhegan River watershed which were suspected as contributing to the flooding, likely had gates open prior to the flood or early in the event, and were not likely to have been important factors," wrote the chief engineer for the New Hampshire Department of Environmental. Among the resulting problems was the bursting of a private earthen dam in south Milford and a stone dam in Hollis that officials broke open because of concern that it would give way. The engineer says more detailed answers may come from a detailed study of flooding on ten rivers in southern New Hampshire.
Source:
http://www.nashuatelegraph.com/apps/pbcs.dll/article?AID=/20080126/NEWS01/476715753/-1/news

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

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

Contact DHS

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

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

Department of Homeland Security Disclaimer