Department of Homeland Security Daily Open Source Infrastructure Report for 4 January 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- The Associated Press reported that on Monday the State Department approved technology, which will allow passport cards to be read from up to 20 feet away. A passport card can be used by U.S. citizens instead of a passport when traveling to other countries in the western hemisphere. Privacy advocates criticized the department for not doing more to protect information on the card, but the State Department said privacy protections will be built into the card. (See items **12**)
- Also according to the Associated Press, prosecutors in Davis County, Utah, are dropping charges against a Hill Air Force Base employee who crafted more than 40 pipe bombs, which were found stashed behind two area businesses. The county says it will dismiss its case in lieu of federal charges that carry stiffer potential penalties. Federal prosecutors have charged the man with one count of possessing improvised explosives devices or bombs and one count of storing explosive material in a manner not in conformity with regulations. (See item **26**)

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 3, BBC News* – (Alaska) **Alaska oil exploration to begin.** The government says it will offer exploration rights for oil and gas in a northwestern region of Alaska.

The federal Minerals Management Service said it would take bids next month for concessions in the Chukchi Sea, which separates Alaska from Siberia. But environmental groups fear the effects on wildlife in the region, including the polar bear population. There have been no lease sales for over 15 years and the groups fear further exploration could damage marine life. Energy exploration in Alaska has always been a tough choice between preserving one of the planet's last great areas of pristine wilderness and the potential for huge profits to be made from its development. The American sectors of the Chukchi Sea are believed to hold 15 billion barrels of recoverable oil and over seven trillion cubic feet of natural gas. But the authorities had not held a lease sale in the sea since 1991, both due to the difficulties and cost involved in extraction from the Arctic continental shelf and concerns over the environment. The Minerals Management Service says exploration will not be allowed to take place any closer than 50 miles from the shoreline, therefore striking a balance between development and protection of coastal resources.
Source: http://news.bbc.co.uk/2/hi/americas/7169144.stm

2. *January 2, Reuters* – (National) **Bush won't release emergency oil to ease prices.** President Bush will not tap the U.S. Strategic Petroleum Reserve (SPR) to ease oil prices that hit a record high of $100 a barrel on Wednesday, the White House said. "This president will not use the SPR to manipulate (oil prices)," a White House spokeswoman said. "Doing a temporary release of the SPR is not going to change prices very much." The spokeswoman said the Bush administration understood that high energy prices hurt family budgets and small businesses, but it believes that using the emergency oil stockpile to lower crude prices is not the solution. "We have to figure out a way to increase supply here in the United States," she said. "The SPR is supposed to be used for emergencies. We know that markets work." The stockpile was created by Congress in 1975 in response to the Arab oil embargo. The reserve now holds about 698 million barrels of crude at four underground storage sites in Texas and Louisiana. The Energy Department said that, despite record high prices, it would not delay oil deliveries to the reserve and will carry out its plan to add 12.3 million barrels of crude to the stockpile during the first half of this year.
Source:
http://news.yahoo.com/s/nm/20080102/us_nm/bush_oil_dc;_ylt=AhEgPhUFgGlwL2U0YIVmrrMWIr0F

[Return to top]

Chemical Industry Sector

3. *January 3, Associated Press* – (Alabama) **Army: More chemical weapons destroyed.** The Army says it is making progress in destroying thousands of chemical weapons stored at the Anniston Army Depot in Alabama. Since December 26, workers have incinerated 3,846 VX-filled 155 millimeter artillery shells and 2,454 gallons of liquid VX. More than 76,000 of the shells and almost 47,000 gallons of the nerve agent have been destroyed since June. Officials say that all munitions filled with nerve agent GB have been eliminated. The figures mean just under 40 percent of the entire chemical weapons stockpile has now been destroyed.

Source: http://www.al.com/newsflash/regional/index.ssf?/base/news-33/1199368793270280.xml&storylist=alabamanews

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

4. *January 3, Free-Lance Star* – (Virginia) **Reactor cooler pump shuts down at North Anna; motor is replaced.** In Virginia, Unit 2 at the North Anna Power Station is being restarted after a pump malfunction shut down the reactor on Christmas Day. "We had a problem with a reactor coolant pump," a spokesman for Dominion power nuclear operations, said yesterday. "The motor was bad, so we had to have another shipped down and installed." There was no danger to plant workers or the surrounding community. The malfunction occurred at 9:10 p.m. December 25 and was reported to the Nuclear Regulatory Commission about two hours later. The pump problem was unrelated to an incident in June, in which Unit 2 was shut down for more than a week. In that case, an electrical circuit malfunction caused a safety-injection water system to start, causing the unit and its main turbine to shut down. The injection system provides cooling water to the reactor core in the event that coolant is lost or depleted. Unit 2 was shut down for nine days, and the event triggered a special inspection by the NRC. The agency found that reactor operators at the plant properly handled the shutdown. Source: http://fredericksburg.com/News/FLS/2008/012008/01032008/345819?rss=local

5. *January 2, Washington Post* – (Virginia) **Uranium lode in Virginia is feared, coveted.** Underneath a plot of farmland used to raise cattle, hay, and timber in south central Virginia lies what is thought to be the largest deposit of uranium in the United States. Now, three decades after the deposit was found, the landowner has set his sights on mining the 200-acre site, despite concerns of environmental groups and residents about unearthed radioactive material that could contaminate the area's land, air, and source of drinking water. The estimated 110 million pounds of uranium in Pittsylvania County, worth almost $10 billion, could supply all of the country's nuclear power plants for about two years. There is a hurdle to clear before an ounce of the element can be mined: It is illegal to mine uranium in Virginia. But the General Assembly is considering changing that. This month, the landowner's company, Virginia Uranium, will try to persuade the General Assembly to take the first step – approving a $1 million study that will explore whether uranium can be safely mined in Virginia. If the study shows that it can be done, the company will ask the legislature to lift a state ban on uranium mining. Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/01/01/AR2008010101811.html

[Return to top]

Defense Industrial Base Sector

6. *January 3, Arizona Daily Star* – (National) **Raytheon wins $232.3M contract.** Raytheon Missile Systems won a U.S. Army contract valued at $232.3 million to develop a precision-guided ammunition round for a new weapon system. Raytheon, the

world's largest missile maker, beat Alliant Techsystems Inc. in bidding for the contract to develop the XM 1111 Mid-Range Munition. The contract builds on Raytheon's success in precision-guided projectiles, which feature tracking sensors hardened to survive firing from traditional artillery platforms. The 120-millimeter, or roughly 4.7-inch diameter, Mid-Range Munition is planned for use on the Future Combat System's Mounted Combat System. The weapon will allow U.S. forces to strike at enemy targets beyond the line of sight, using an infrared imaging sensor and a digital, semi-active laser seeker developed and successfully demonstrated during a two-year Army program.
Source: http://www.azstarnet.com/sn/business/218861.php

[Return to top]

Banking and Finance Sector

7. *January 3, Tulsa World* – (Oklahoma) **Latest telephone scam targets older Oklahomans.** Telephone calls asking primarily older Oklahomans to provide bank account information or risk losing their Medicaid or SoonerCare benefits are a scam, officials said Wednesday. The callers tell people that they no longer will be eligible for Medicaid unless they give their bank account information, said the vice president of the Oklahoma Bankers Association's Fraud Division in Oklahoma City. The Health Care Authority has teamed with the Oklahoma Bankers Association to identify the scam and help people avoid becoming targets, he said. The Oklahoma Health Care Authority or SoonerCare will never call participants to ask for bank account numbers or other financial information over the phone, said a spokesman for the agency.
Source:
http://www.tulsaworld.com/news/article.aspx?articleID=20080103_1_A9_spanc07146

8. *January 2, Washington Post* – (National) **Online records may aid ID theft.** The Federal Trade Commission has estimated that 8.3 million Americans were victims of identity theft in 2005, the most recent data available. Despite this, Social Security numbers can be mined easily in the government's own records and are readily available in many courthouses -- in land records and criminal and civil case files -- as well as on many government Web sites that serve up public documents with a few clicks of a mouse. From state to state, and even within states, there is little uniformity in how access to the private information in these records is controlled. A recent spot-check found the nine-digit numbers on hundreds of land deeds, death certificates, traffic tickets, creditors' filings, and other documents related to civil and criminal court cases. Federal courts have banned the numbers from appearing on public documents since 2001. And in recent years, many jurisdictions, including Virginia, Maryland, and the District, have enacted laws or made rules barring various types of personal information from being filed with courts or government agencies. Most court Web sites in the Washington, DC, region list partial Social Security numbers or none at all. However, millions of paper records were filed across the U.S. before the laws and rules took effect. Generally, such records are not covered by the prohibitions. And court clerks said it would be virtually impossible to redact all of the Social Security numbers in them. In Loudoun County, Virginia General District Court, Social Security numbers were found on documents filed in 38 of the 48 criminal cases heard by a judge on a recent day. The

numbers were typed or written on summonses, arrest warrants, criminal complaints, and jail commitment and release orders, among other documents.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/01/01/AR2008010102334.html?nav=rss_business

9. *January 2, News Herald* – (Florida) **Bay Bank and Trust customers targeted in scam.** The Bay County Sheriff's Office has received several complaints from citizens who received recorded messages from someone claiming to be with Bay Bank and Trust. The person states that because of the New Year, the bank is checking customer information and requests the recipient dial another number to give updated information. A call to that number Wednesday revealed an automated voice that promised customers "enhanced card security" and said the information was needed because Bay Bank was "protecting you from fraud and identity theft." The calls appear to be made at random, as some of the recipients do not have an account with Bay Bank and Trust, said a Sheriff's Office spokeswoman.
Source: http://www.newsherald.com/headlines/article.display.php?id=173

10. *January 2, KTRV 12 Boise* – (Idaho) **FBI warns of new scam.** The FBI is warning Idahoans about a scam in which someone who claims to be a police officer tells victims they have failed to show up for jury duty and there is a warrant out for their arrest. The caller often asks for your birth date and social security number for verification purposes. In some cases, the scammer even says there is a monetary solution, payable by credit card. The local Better Business Bureau says this is a common ploy.
Source: http://www.fox12news.com/Global/story.asp?S=7569588

[Return to top]

Transportation Sector

11. *January 3, Boston Globe* – (Massachusetts) **Bridge rebuilding may snag Centre.** An impending MBTA bridge reconstruction project could close a key route in and out of the business district of Newton for much of 2008, officials said. The Massachusetts Bay Transportation Authority has determined that rebuilding the 100-year-old Langley Road Bridge is a top safety priority and is prepared to begin the reconstruction effort this spring. Situated on the southeast edge of the business district, the bridge allows Green Line trolleys on the MBTA's Riverside Line to pass underneath Langley Road as they pull in and out of Newton Centre Station. Langley Road is a heavily traveled route between Newton Centre and Route 9. MBTA officials said the design work for the $2.3 million project is complete, and construction, with its diversion of traffic, is expected to begin in May. Officials recently determined that replacing the bridge - built in 1907 and last rebuilt in 1959 - would be more cost-effective than trying to repair and maintain it any longer, they said. Local residents and politicians expect the project to have an adverse affect on traffic and area businesses.
Source: http://www.boston.com/news/local/articles/2008/01/03/bridge_rebuilding_may_snag_centre/

12. *January 2, Associated Press* – (National) **Passport card technology approved.** On Monday the State Department approved technology that will allow passport cards, which can be used by U.S. citizens instead of a passport when traveling to other countries in the western hemisphere, to be read from up to 20 feet away. This process only takes one or two seconds. The card would not have to be physically swiped through a reader, as is the current process with passports. Privacy advocates criticized the department for not doing more to protect information on the card, but the State Department said privacy protections will be built into the card. The chip on the card will not contain biographical information. A 2004 law to strengthen border security called for a passport card that frequent border crossers could use that would be smaller and more convenient than the traditional passport. Currently, officials must swipe travelers' passports through an electronic reader at entry points.
    Source: http://news.yahoo.com/s/ap_travel/20080102/ap_tr_ge/travel_brief_security;_ylt=App.sf6YhN2c6j.7FoEOaoes0NUE

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture and Food Sector

13. *January 2, Associated Press* – (Minnesota) **Minnesota Tests Bovine TB.** Minnesota animal health officials have completed testing 1,500 of the state's cattle herds for bovine tuberculosis and have found no new cases. The Board of Animal Health says the sample was big enough to conclude that the disease is not widespread in the state. It has only been found in the northwest corner. Testing started in September 2006 as part of a plan to eliminate the disease from the state's livestock and wildlife populations. Minnesota cannot apply to the federal Agriculture Department for accreditation as TB free until two years after its last infected herd is eliminated. Without the TB-free designation, it costs ranchers about $10 for additional testing for every animal they ship out of state. Testing will continue in northwest Minnesota.
    Source: http://www.chron.com/disp/story.mpl/ap/fn/5420543.html

14. *January 2, theHorse.com* – (National) **USDA releases annual animal health report.** The U.S. Department of Agriculture has released the 2006 U.S. Animal Health Report, a national overview of domestic animal health in the U.S. It addresses the many components of the country's animal health infrastructure, including: approaches to animal disease surveillance, control, and eradication; animal population demographics; and new initiatives. The report also describes significant epidemiologic events during the year. Readers will also find a chapter on animal health research underway by collaborating agencies within USDA and U.S. schools of veterinary medicine. Also new this year is a chapter on international collaboration and capacity-building projects. This

chapter describes numerous training, educational, and outreach programs underway to safeguard and improve animal health globally. The report is available online at: http://www.aphis.usda.gov/publications/animal_health/content/printable_version/06_AHReport_508.pdf.
Source: http://www.thehorse.com/ViewArticle.aspx?ID=11093

[Return to top]

Water Sector

15. *January 2, WaterTechOnline* – (New Hampshire) **MTBE found in many New Hampshire wells.** A fair portion of New Hampshire's groundwater contains the gasoline additive MTBE (methyl tertiary-butyl ether), but almost all of its concentrations are below both the state's drinking water limit and the federal government's advisory limit, according to a new U.S. Geological Survey study, results of which were announced in a January 2 press release. MTBE was introduced nationally into gasoline in 1979 as an octane booster that would substitute for lead. It was mandated for four New Hampshire counties in 1995 to provide cleaner-burning gasoline, but not in the rest of the state, according to USGS. A number of states have now banned it in gasoline, but USGS says no data exist on the human health effects of ingesting MTBE in drinking water. Across the state, more than 70 percent of wells serving mobile home communities had MTBE, USGS said.
Source: http://watertechonline.com/news.asp?N_ID=68898

[Return to top]

Public Health and Healthcare Sector

16. *January 3, New York Times* – (National) **Hospitals slow in heart cases, research finds.** In nearly a third of cases of sudden cardiac arrest in the hospital, the staff takes too long to respond, increasing the risk of brain damage and death, a new study finds. The study, which was published Thursday in the New England Journal of Medicine, was based on the records of 6,789 patients at 369 hospitals, whose hearts stopped because of conditions that could be reversed with an electrical shock from a defibrillator. When the defibrillation was delayed, only 22.2 percent of patients survived long enough to be discharged from the hospital, as opposed to 39.3 percent when the shock was given on time. Delays were more likely in patients whose hearts stopped at night or on the weekend, who were admitted for noncardiac illnesses, in hospitals with fewer than 250 beds, and in units without heart monitors. While exact numbers are not known, researchers estimate that 370,000 to 750,000 hospitalized patients have a cardiac arrest and undergo resuscitation every year in the United States. In a third to half, the arrest is caused by an abnormal, too-fast rhythm that can be corrected with a shock.
Source: http://www.nytimes.com/2008/01/03/health/research/03heart.html?hp

17. *January 3, Agence France-Presse* – (International) **Israel probes new bird flu outbreak.** "This morning, 18 ducks, chickens and pigeons were found dead among a total of 25 birds held in a petting corner in a kindergarten in Binyamina," an agriculture

ministry spokesman said. Tests discovered the presence of the H5 virus category, which only kills birds, unlike the highly pathogenic H5N1 sub-type of the virus that is dangerous to humans. Experts were examining the infected birds to see if they had been infected with the H5N1 strain. Authorities have banned the transportation of animals in a two-mile radius around Binyamina, a coastal town north of Tel Aviv, in a bid to prevent the spread of the virus, the agriculture ministry said in a statement.
Source: http://www.breitbart.com/article.php?id=080103131947.sl1rucnu&show_article=1

Government Facilities Sector

Nothing to report.

[Return to top]

Emergency Services Sector

18. *January 2, National Counterterrorism Center* – (National) **NCTC releases 2008 Counterterrorism Calendar.** The National Counterterrorism Center (NCTC) today announced the release of its 2008 counterterrorism calendar. The calendar is now available in print and via NCTC's website at: http://www.nctc.gov in both a downloadable PDF and an online, interactive version. NCTC has published a "daily planner" print version of its counterterrorism calendar since 2005. This year's calendar is the largest ever, with 160 pages of information on known terrorist groups, individual terrorists, and technical information on topics such as biological and chemical threats. The interactive online version of the calendar provides the public with user-friendly access to the same information, with the addition of locator maps, photographs, and lists of helpful links specific to each threat area. An NCTC spokesperson said, "The NCTC 'daily planner' version of the calendar is a prized resource for law enforcement and national security personnel, providing easy access to terrorist profiles and information on terrorist groups. The calendar also provides invaluable first-responder information on biological threats, chemical agents, medical symptoms of nerve agent exposure, and more. Our new, interactive calendar provides easier, broader access to this information, and should serve as a valuable research tool for emergency services providers, government personnel, and the general public."
Source: http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/01-02-2008/0004729564&EDATE

[Return to top]

Information Technology

19. *January 2, Computerworld* – (National) **'Ransomware' extorts payment with phone call.** New "ransomware" that locks up a person's PC and demands $35 to return control to its user is on the prowl, a security researcher said this week. The extortionists tell

victims of the Delf.ctk Trojan horse to dial a 900 number, said the CEO of Sunbelt Software Distribution Inc., a Clearwater, Florida-based security developer. That number can be traced to "passwordtwoenter.com," a payment processor also used by hardcore pornography Web sites to charge for access to their content, he added. Users infected with the Trojan horse see a full-screen message posing as an error generated by Windows, according to screenshots posted on the Sunbelt company blog on Monday. "ERROR: Browser Security and Antiadware [sic] Software component license exprited [sic]," the message reads. "Surfing PORN, ADULT and some other kind of sites you like without this software is dangerows [sic] and threatens with infection of your computer by harmful viruses, adware, spyware, etc." The bogus update window includes a "Click to activate new license" button that in turn brings up another screen, this one telling U.S. users to dial a 900 telephone number and enter a personal identification number (PIN). If the 900 number does not work, the page instructs users to dial alternate numbers -- one in the West African nation of Cameroon, the other a satellite telephone number. "You're completely locked out of the system" after the Delf.ctk Trojan horse installs and runs, said Sunbelt. The only way to regain control is to pay up by dialing. Ransomware, a term used to describe malware that tries to extort money from users after an infection -- usually to return access to suddenly-encrypted files -- is rare, but not unknown. The last outbreak of any note was in July 2007, when another Trojan horse, dubbed "GpCode," demanded $300 to unlocked frozen files.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9054867&taxonomyId=17&intsrc=kc_top

20. *January 2, Network World* – (National) **'Diehard' virus variants flexing muscle.** New Windows-based "downloader" malware known as Trojan-Downloader.Win32.Diehard has surged to the top of Kaspersky Lab's "Virus Top Twenty" list for December because of its "explosive propagation," the security firm said Wednesday. A downloader is a type of malware, which once loaded onto a victim's machine, can enable the attacker to download many other types of malicious code to exploit and control it for activities ranging from spam to information theft. The worst virus of the month in terms of sightings was not the Diehard downloader, but a variant on the old NetSky, the worm that is still spreading almost four years after being discovered. Kaspersky reckons that the NetSky.q worm surged to 20 percent of e-mail traffic last month. But the real surprise for December, according to Kaspersky, was that the Diehard variants grabbed the second, fourth, and seventh spots on its list. This was a surprise because the .dc modification variant, which grabbed the second-place ranking, first appeared only on December 21. But within a matter of days it constituted an estimated 80 percent of all malicious traffic for the month. Two other Diehard variants grabbed fourth and seventh place in December. In its own findings, Kaspersky Labs stated that the significance is that "classic e-mail worms" may still rank high, but they tend to quickly disappear, only "creating a backdrop for the real battle which is taking place," which is "Trojan programs and phishing attacks." Security firm Akonix, which specializes in instant-messaging (IM) based defense, today said it counted three new IM-based worms in December — Cargar, Etest, and YMWorm — and determined that there have been a total of 346 IM-targeted malware types for 2007, down from the 406 IM malware types

seen in 2006.
Source: http://www.networkworld.com/news/2008/010208-diehard-virus.html

21. *January 2, Dark Reading* – (National) **Breaches plague government agencies.** Two more major losses of private data have been reported by government agencies in the past few days, adding fuel to fiery criticism of federal and regional government's privacy practices over recent weeks, both in the U.S. and overseas. A holiday break-in at the Davidson County Election Office in Tennessee resulted in the theft of two laptops containing personal information on all 337,000 voters in the region, according to reports. The data included full Social Security numbers for each voter, and at least one report indicated that the data was not encrypted. Meanwhile, more than 10,000 U.S. Air Force active and retired employees were informed Friday that a laptop containing their Social Security numbers, birth dates, addresses, and telephone numbers is missing, according to reports. The laptop belonged to an Air Force band member at Bolling Air Force Base in Washington, D.C., and was reported missing from his home. A stolen laptop containing personal information was also reported by the Minnesota Department of Commerce on Friday. The data losses by the regional and federal government agencies in the U.S. are fuel to the fire of criticism that has taken place in the U.K. over the past several weeks, as more details come to light about breaches in several British government agencies. Criminals may not even have to break in or steal data to get citizens' personal information from government agencies, according to a report in yesterday's Washington Post. The report notes that criminals can gather names, Social Security numbers, and other personal data simply by scanning through online public records and documents.
Source: http://www.darkreading.com/document.asp?doc_id=142215&WT.svl=news1_1

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

22. *January 3, Associated Press* – (Wisconsin) **Teen gets jail term for cutting Internet service.** A teen accused of hacking into a computer system and shutting down Internet access to Marshfield, Wisconsin, for 18 hours has been sentenced to a 90-day jail term. The 18-year-old was granted work release privileges as part of his jail sentence on a charge of entering a computer system and causing damage. He also was ordered to serve three years probation and pay restitution of just under $6,000. The criminal complaint said the Berlin, Wisconsin, resident attempted last April 25 to gain access to a control console interface at a Solarus computer system station in Marshfield. The first attempt failed, but an attempt two minutes later was successful. When he turned off a router

controlling Internet for customers in the Marshfield area, the system went down for about 18 hours and also sustained damage.
Source: http://www.todaystmj4.com/news/local/13004667.html

23. *January 2, Ars Technica* – (National) **WiFi flu: Viral router attack could hit whole cities.** According to a paper written by a team of researchers at Indiana University, an attack that specifically targets wireless routers and spreads between them at any point where coverage overlaps could quickly and easily propagate throughout an entire city. Until recently, such an attack vector was considered unlikely. Wireless routers are inherently less secure than their wired counterparts, but the development of WPA encryption has increased (theoretical) wireless security significantly. More practically, wireless routers were not deployed in sufficient numbers and did not overlap their areas of coverage enough to present a significant propagation risk. As the density and scale of wireless coverage has expanded, however, the chance that a router-focused viral attack could cause significant damage has increased. The IU team's goal was to map existing real-world wireless networks in various urban locations. Once this was done, the researchers simulated how quickly an infection would spread across the various networks tested and what general steps could be taken to prevent such attacks or reduce their severity. Modeled locations included Chicago, Boston, New York City, the San Francisco Bay area, Seattle, and both northern and southern Indiana. The data gathered from each area was then used to map the growth of a hypothetical viral infection. Although the areas modeled differed considerably in size, composition, and geography, all of them demonstrated a sharp initial infection rate as the virus spread across non-encrypted routers. By the time the infection phases had run their course, 10-55 percent of the routers in the measured area were controlled by malware. Such findings speak to the importance of strong security measures. Even if a minority of routers in any given area is using WPA, strategic positioning of such routers can prevent malware from escaping what becomes an effectively isolated area. To date, there have been no known attempts to attack a wireless network in this manner, but the increasing ubiquity of wireless connectivity makes such attacks almost inevitable. (For the PDF version of the Indiana report, see: http://arxiv.org/PS_cache/arxiv/pdf/0706/0706.3146v1.pdf.)
Source: http://arstechnica.com/news.ars/post/20080102-wireless-router-security-flaws-could-fuel-viral-outbreak.html

24. *January 2, KLAS 8 Las Vegas* – (Nevada) **Explosive device disrupts phone service.** Residents in the northeast area of the Las Vegas Valley were without phone service while repair crews work on a transmitter that was damaged by an explosive device. Residents told police they heard an explosion around 3 a.m. Wednesday. Las Vegas police, the FBI, and ATF were on the scene investigating. Phone service was expected to be out until Wednesday evening.
Source: http://www.lasvegasnow.com/Global/story.asp?s=7568343

[Return to top]

Commercial Facilities Sector

25. *January 3, Oxford Press* – (Ohio) **Police: Gunpowder-filled pipe source of deadly**

explosion. The blast that killed a West Chester Township, Ohio, teen Wednesday afternoon came from a pipe filled with gunpowder, according to police. He was nearly 110 feet away from the explosion, according to a Police Department official. Two juveniles were transported to the Butler County Juvenile Detention Center for involvement in the explosion.
Source: http://www.oxfordpress.com/hp/content/oh/story/news/local/2008/01/03/HJN010408explosionfolo.html

26. *January 2, Associated Press* – (Utah) **Davis County drops pipe bomb charges, will let feds prosecute.** Davis County, Utah, prosecutors are dropping charges against a Hill Air Force Base employee who crafted more than 40 pipe bombs found stashed behind two area businesses. The county says it will dismiss its case in lieu of federal charges that carry stiffer potential penalties. Forty bombs stolen from a Clearfield storage unit owned by the man were found behind a Layton car wash on September 5. Five days later at least four more bombs were found behind a Roy convenience store. Federal prosecutors have charged the man with one count of possessing improvised explosives devices or bombs and one count of storing explosive material in a manner not in conformity with regulations.
Source: http://origin.sltrib.com/news/ci_7862715

27. *January 2, Associated Press* – (International) **State Department issues list of threats U.S. businesses face.** U.S. businesses faced varied threats in 2007 — including cyberattacks in Europe, theft of intellectual property in Asia, natural disasters in Latin America, terrorism on many continents — according to a year-end analysis by the U.S. State Department's Overseas Security Advisory Council. In Europe, two weeks of attacks by computer interlopers that crippled government and corporate Web sites beginning in late April raised a new worry that U.S. companies also could be vulnerable to attack by computer. Among 10 security issues cited in the report, the council also warned of rising homegrown political radicalism and terrorism in Europe. Intellectual property theft, terrorism, natural disasters, and political instability were listed as the most serious security challenges in Asia. The threat from fraud and theft of trade secrets has been rising exponentially, the report said. It cited China and India as countries of greatest concern and warned that much of the damage comes from within companies.
Source: http://www.buffalonews.com/145/story/241556.html

[Return to top]

National Monuments & Icons Sector

Nothing to report.

[Return to top]

Dams Sector

28. *January 3, Grand Forks Herald* – (Minnesota) **DNR set to present Lake Bronson**

Dam options. Officials are planning a public meeting at the end of this month to discuss the Lake Bronson Dam, which recently was named the most dangerous in the state by the Minnesota Department of Natural Resources. The dam holds back about 313 acres of water collected from a 400-square mile watershed to the north. Officials say the 70-year-old dam is deteriorating quickly and presents a safety hazard to the same downstream communities it benefits. The DNR has concurred, deeming the dam to be "high hazard," the only dam owned by the state with that designation. A representative from the DNR Division of Parks and Recreation said he expects 13 to 15 alternatives will be presented at the public meeting. "It will have everything from do nothing to the total removal of the dam," he said, but a middle course is more likely. "Doing nothing really is not a possibility because we have some real safety concerns there and removing the dam defeats the purpose of having a park there."
Source:
http://www.grandforksherald.com/articles/index.cfm?id=62484&section=news&cid=0

[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
Subscription and 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