Department of Homeland Security Daily Open Source Infrastructure Report for 16 January 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- KGTV 10 San Diego reported that an employee at the San Onofre nuclear power plant in San Diego falsified records for five years to show that hourly fire patrols were made, when in fact they were not. This has led the U.S. Nuclear Regulatory Commission to order Southern California Edison to make changes, including developing special safety training. (See items **6**)
- According to the ASU Web Devil, a group of professors received approximately $263,800 from the National Center for Food Protection and Defense to research the possibility of agro-terrorism, or terrorists contaminating fruits and vegetables, coming through the border at Nogales. Members of the group will be traveling to Nogales to work with Mexican authorities to finalize the survey next month. The study will run through May 2009. (See item **16**)

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 15, Associated Press* – (International) **Bush: OPEC nations should pump more oil.** President Bush urged OPEC nations on Tuesday to put more oil on the world market and warned that soaring prices could cause an economic slowdown in the United States. “High energy prices can damage consuming economies,” the president told a

small group of reporters traveling with him in the Mideast. "It's affected our families. Paying more for gasoline hurts some of the American families, and I'll make that clear to him," said Bush, heading into more talks with the Saudi King. Shortly after Bush spoke, the Saudi oil minister said the kingdom, responsible for almost one-third of the cartel's total output, would raise oil production when the market justified it. The Organization of Petroleum Exporting Countries next meets February 1 in Vienna, Austria, to consider increasing output. OPEC oil accounts for about 40 percent of the world's needs, and OPEC ministers often follow the lead of the Saudis when discussing whether to increase production to take the pressure off rising prices.
Source: http://news.yahoo.com/s/ap/20080115/ap_on_re_mi_ea/bush_mideast

2. *January 15, Casper Star-Tribune* – (Northwest) **Big pipeline gives Wyoming a boost.** The second phase of the Rockies Express natural gas pipeline to the Midwest is complete, although some "off-ramps" on the eastern end are not yet open. "The freeway is finished, but not all of the exits," said the executive director of the Wyoming Pipeline Authority. The 1,663-mile Rockies Express pipeline is one of the largest natural gas pipelines ever constructed in North America and will transport natural gas from prolific producing basins in Wyoming and Colorado to the upper Midwest and eastern United States, according to developers Kinder Morgan and Sempra Energy. When completed, the $4.4 billion project will transport up to 1.8 billion cubic feet of gas per day. Rockies Express represents a lifeline for Wyoming's natural gas industry, which provides about one-third of state government revenue. Rising gas production in the Rockies approached pipeline export capacity and drove prices well below the national average in 2007. So far, completion of Rockies Express pipeline's second phase has added about 900 million cubic feet per day of export capacity for the region, helping lift wholesale prices closer to the national average. Completion of several more "off-ramps" to the segment in February should add another 500 million cubic feet of daily capacity. That is enough to serve about 18,000 homes for a year.
Source:
http://www.casperstartribune.net/articles/2008/01/15/news/wyoming/dc9b3a68f1118ed5872573d10003bd30.txt

[Return to top]

Chemical Industry Sector

3. *January 15, WLKY 32 Louisville* – (Kentucky) **Explosions reported at chemical plant.** Two explosions have been reported at a west Louisville chemical plant. The plant has been evacuated. Area residents have not been evacuated, but they have been advised to stay indoors. A fire department spokesman said a pigment made by the company is leaking and that nearby residents are being asked to stay inside. He also said rail traffic near the plant has been shut down. Calls to company officials were not immediately returned.
Source: http://www.wlky.com/news/15052645/detail.html

4. *January 14, United Press International* – (Massachusetts) **MIT creates tiny gas sensor.** U.S. engineers are developing a tiny sensor that can detect minute amounts of gases,

including toxic industrial chemicals and chemical warfare agents. Massachusetts Institute of Technology researchers said they have taken the common techniques of gas chromatography and mass spectrometry and shrunk them to fit into a device the size of a computer mouse. Eventually, the team, led by an MIT Professor, plans to build a detector about the size of a matchbox.
Source:
http://www.upi.com/NewsTrack/Science/2008/01/14/mit_creates_tiny_gas_sensor/7629/

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *January 15, Washington Post* – (National) **Nuclear safety rule ignites strong reactions.** Federal regulators approach to solving one of the United States' biggest post-September 11 fears – a terrorist flying a plane into a nuclear power plant – is under attack for adding to public safety concerns. Comments filed with the Nuclear Regulatory Commission last month said the agency's October 3 proposal, which directs that only some new plant designs be assessed for risk to air attack, did not go far enough. "By requiring only a limited subset of anticipated new reactors (less than half of the currently announced plants) to address aircraft impacts as part of the design, the NRC's proposed rule could undermine public confidence in new nuclear power plants," according to the president and chief executive of Unistar Nuclear Energy of Baltimore. Public acceptance of plant safety is considered critical to the rebirth of the nuclear industry, where there has been a de facto moratorium on new construction since the Three Mile Island accident in 1979. The 104 existing reactors, which supply 20 percent of U.S. electricity, are not covered by the proposed rule.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/01/14/AR2008011402576.html

6. *January 14, KGTV 10 San Diego* – (California) **San Onofre Nuclear Plant caught falsifying records.** An employee at the San Onofre nuclear power plant in San Diego falsified records for five years to show that hourly fire patrols were made, when in fact they were not, the U.S. Nuclear Regulatory Commission announced Monday. The finding prompted the NRC to order Southern California Edison (SCE), which is the majority owner of the San Onofre Nuclear Generating Station, to make changes, including developing special safety training. The order requires SCE to expand its ethics training for managers, supervisors, and employees; develop new training to prevent deliberate misconduct; conduct an independent safety culture assessment; and monitor the effectiveness of its corrective actions. According to the NRC's investigation, a fire protection specialist at the San Onofre nuclear plant provided inaccurate information about hourly fire watch rounds the staffer was supposed to make while working the midnight shift at the plant from April 2001 to December 2006.
Source: http://www.10news.com/news/15047670/detail.html

[Return to top]

Defense Industrial Base Sector

7. *January 14, Centre Daily Times* – (National) **URS awarded Air Force flight training contract.** URS Corporation announced that the Company's EG&G Division has been selected by the U.S. Air Force's Air Education and Training Command to support its Undergraduate Flight Training (UFT) program. The re-compete contract includes a one-year base period and five one-year options periods. The maximum value of the contract to URS is $267 million over the full six years. Under the terms of the contract, URS will provide courseware development, simulator, and academic instruction for the T-1, T-6, T-37, and T-38 aircraft, as well as combat systems officer training, in support of the UFT program.
   Source: http://www.centredaily.com/business/story/331774.html

[Return to top]

Banking and Finance Sector

8. *January 14, WJHG 7 Panama City* – (National) **Another scam to worry about.** Walton county officials are warning about a new scam that has victimized people in Texas, Alabama, Indiana, Tennessee, Wisconsin, and Florida. The company, Guildan Management Group of Salt Lake City, places ads in the local newspapers and on the internet telling how it can help people get cash loans. The victims submit the "loan application" and are notified that they are approved. They are instructed to wire an advanced fee called "loan or credit insurance" to an individual in Canada. That is the last the victims see of their money. And, the company's Salt Lake City address is a fake. Investigators are warning people about the scam, and advising them to go through their local banks for recommendations about legitimate lenders.
   Source: http://www.wjhg.com/news/headlines/13777262.html

9. *January 14, Security Pro News* – (National) **Nigerian spam restitution latest scam attempt.** Security vendor Symantec said in its State of Spam report for December 2007 that something new showed up with the usual assortment of holiday-related junk email. A restitution offer promised to reimburse people victimized by 419 scams. "The scam states that payments will be supervised by U.N. officials and about 150 scam victims will be paid compensation of $100,000 each," Symantec said of the spam. "It provides some URL links as a reference to money that was successfully recovered by 419 scam victims." "At the bottom of the email, it explains how the money may be recovered and the fraudulent background of such emails may be observed." In keeping with the times, spam based on the ongoing Presidential primary campaigns has been spotted. These purport to give a reward, like a $500 gift card, in exchange for their opinion on Hillary Clinton's electability. However, the destination for these sites collects personal information, with no reward provided for doing so.
   Source: http://www.securitypronews.com/news/securitynews/spn-45-20080114NigerianSpamRestitutionLatestScamAttempt.html

10. *January 14, IDG News Service* – (Tennessee) **Nashville laptop theft may cost $1**

million. The theft of a laptop containing Social Security numbers of Nashville, Tennessee-area voters is expected to cost local officials about $1 million as they provide identity-theft protection to those affected. County officials say that thieves broke into Davidson County Election Commission offices on the weekend before Christmas, smashing a window with a rock and then making off with a $3,000 router, a digital camera, and a pair of Dell Latitude laptops containing names and Social Security numbers of all 337,000 registered voters in the county. County election officials began notifying residents of the breach on January 2, and the local government is offering victims one year of free identity theft protection from Debix Identity Protection Network. The price tag for the laptop theft is expected to be in the $1 million range. Since state data breach disclosure laws went into effect a few years ago, the theft of an unencrypted laptop computer can become a major problem for any organization that stores sensitive data.
Source: http://www.infoworld.com/article/08/01/14/Nashville-laptop-theft-may-cost-1-million-dollars_1.html

[Return to top]

Transportation Sector

11. *January 15, Associated Press* – (National) **Panel: Increase gas tax to fix roadways.** A two-year study released Tuesday by the National Surface Transportation Policy and Revenue Study Commission warns that urgent action is needed to ease traffic congestion and repair the nation's decaying bridges and roads to avoid future disasters. Under the recommendation, the current tax of 18.4 cents per gallon for unleaded gasoline would be increased annually for five years -- by anywhere from 5 cents to 8 cents each year -- and then indexed to inflation afterward to help fix the infrastructure, expand public transit and highways as well as broaden railway and rural access, according to persons with direct knowledge of the report. The report also calls for rebuilding and expanding the national rail network to meet a growing demand for alternatives to congested highways. But the 12-member commission's proposals, which are expected to cost $225 billion each year for the next 50 years, face internal division. The commission's chairwoman, who is the Transportation Secretary, and two other members oppose gas tax increases and were issuing a dissenting opinion to the report calling instead for private-sector investment and tolls. The commission was formed by Congress in 2005 to study the future needs of the nation's surface transportation system, as well to recommend funding options.
Source: http://www.cnn.com/2008/POLITICS/01/15/transportation.safety.ap/index.html

12. *January 15, USA Today* – (Minnesota) **Plates focus of Minnesota bridge collapse probe.** Federal investigators have concluded that steel plates on the interstate bridge that collapsed last summer in Minneapolis were inadequate to hold the structure together and appear to have been what allowed it to fail, two officials familiar with the investigation said Monday. The National Transportation Safety Board (NTSB) called Tuesday for states to perform safety assessments on the gusset plates in steel girder bridges any time they add weight to a bridge, the sources said. Gusset plates are flat steel structures used to bolt together the steel girders that carry the weight of a bridge. Bridge engineers

typically design the plates to be far stronger than the girders because if one fails, the whole bridge will collapse. In the wreckage of the I-35W bridge, investigators found 16 gusset plates that were fractured, said one of the officials. Eight of the plates were in the location on the south side of the bridge where the collapse began, according to that official. Design changes in 1977 and 1998 added additional pavement and concrete barriers that increased the weight of the Interstate 35W bridge in downtown Minneapolis. The sources said the NTSB has many months of investigation before it can declare what caused the collapse, but the investigation is now focused on the plates.
Source: http://www.usatoday.com/news/washington/2008-01-14-Bridge_N.htm

13. *January 14, Orlando Sentinel* – (Florida) **Suspicious device found outside OIA maintenance hangar.** A suspicious device found outside of the Continental Airlines maintenance hangar at Orlando International Airport (OIA) halted traffic and forced an evacuation for several hours Monday night as officials investigated, according to OIA officials. The package was found by an Orlando police officer on routine patrol in an un-secured parking lot. Several agencies, including Orlando Fire Department's bomb squad, responded to the scene, said an OIA spokeswoman. The device was destroyed by the fire department and the pieces of the device will be sent to a crime lab for further investigation. No one was injured. The device did not affected flights or passengers, she said.
Source: http://www.orlandosentinel.com/news/local/orange/orl-bk-oia011407,0,6497262.story?coll=orl_tab01_layout

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture and Food Sector

14. *January 15, Argus Leader* – (South Dakota) **State health officials tracking salmonella.** The South Dakota Department of Health noted an increase in salmonella cases in December and alerted consumers to practice food safety precautions. Since that announcement, additional cases of the same strain have been reported in three other states, said the state epidemiologist. A total of 171 cases had been reported in South Dakota for 2007, compared to the five-year median of 133 cases a year. For more information, see the department Web site at: http://doh.sd.gov/DiseaseFacts/Salmonellosis.aspx or the CDC Web site at http://www.cdc.gov/ncidod/diseases/submenus/sub_salmonella.htm.
Source: http://www.argusleader.com/apps/pbcs.dll/article?AID=/20080115/NEWS/801150304/1001

15. *January 14, theTrumpet.com* – (International; National) **Plunging grain supply up**

against soaring demand. Analysts see export sales of U.S. wheat "beginning to look like panic buying" as inventories hit record lows. Grain is quickly becoming one of the world's hottest commodities as it sinks into short supply, according to a new publication titled "Panic Buying of Agricultural Sector as Global Grain Inventories Hit Record Lows." Wheat hit over $10 a bushel in the futures market last month, and rice also set a new all-time record. Soybeans hit a 34-year high, and corn was at a nine-month peak. The Canadian Wheat Board reported that wheat prices will remain high, pointing to low global inventories of the grain as the cause. Meanwhile, last month officials forecasted that wheat supplies in the U.S., which is the world's largest wheat exporter, will hit a 60-year low. Soybean stocks are expected to decline 68 percent from last year, and Goldman Sachs has adjusted its 12-month forecast from $9 a bushel to $14.50. Corn may rise from $4.40 a bushel to $5.30 a bushel. Rice, a crucial staple for half of the world's population, is near a 20-year high. Low stockpiles have many grain importers worried. Despite increased wheat prices, demand for American wheat exports is high. "Overseas buyers are purchasing grain, anticipating the U.S. will run out of wheat. Analysts claim this may happen in the market for hard red winter and white wheat. Wheat exports "simply can not be sustained at current levels' according to agricultural experts" At the same time, Russia and China are taking export cap, levy, and tariff measures to restrict outflows of their grain.
Source: http://www.thetrumpet.com/index.php?q=4689.2954.0.0

16. *January 14, ASU Web Devil* – (International; National) **In fruits and vegetables, a terrorist threat lurks.** New research at Arizona State University's Morrison School of Management and Agribusiness is examining how safe food imported from Mexico is. A group of five professors received approximately $263,800 from the National Center for Food Protection and Defense — an agency under the Department of Homeland Security. The money will be used to research the possibility of agro-terrorism, or terrorists contaminating fruits and vegetables, coming through the border at Nogales. Members of the group will be traveling to Nogales to work with Mexican authorities to finalize the survey next month. The study will run through May 2009. The supply chain at Nogales is especially important for the economy, one researcher said. Between October and May, almost half of the produce coming from Mexico to the U.S. passes through its security checkpoints. Approximately 900 trucks of food cross the border every day.
Source: http://www.asuwebdevil.com/issues/2008/01/14/news/703058

[Return to top]

Water Sector

Nothing to report.

[Return to top]

Public Health and Healthcare Sector

17. *January 15, Reuters* – (International) **Plague a growing but overlooked threat.** Plague, the disease that devastated medieval Europe, is re-emerging worldwide and poses a

growing, but overlooked threat, researchers warned on Tuesday. While it has only killed some 100 to 200 people annually over the past 20 years, plague has appeared in new countries in recent decades and is now shifting into Africa, where there have been "major outbreaks," said ecologists at the University of Liverpool. A bacterium known as Yersinia pestis causes bubonic plague, known in medieval times as the Black Death, and the more dangerous pneumonic plague, spread from one person to another through coughing or sneezing. Globally the World Health Organization reports about 1,000 to 3,000 plague cases each year, with most in the last five years occurring in Madagascar, Tanzania, Mozambique, Malawi, Uganda, and the Democratic Republic of Congo. The United States sees about 10 to 20 cases each year. More worrying is that outbreaks seem to be on the rise after years of relative inactivity in the 20th century. The most recent large pneumonic plague outbreak comprised hundreds of suspected cases in the Democratic Republic of Congo in 2006.
Source: http://news.yahoo.com/s/nm/20080115/sc_nm/plague_threat_dc

Government Facilities Sector

18. *January 14, Associated Press* – (International) **FBI: U.S., Canadian terror suspects met in '05.** Two U.S. citizens accused of plotting to attack civilian and government targets shot "casing videos" of Washington landmarks, later found on a terrorism suspect's computer in Britain, and met with suspects in a Canadian terrorism case, an FBI agent testified Monday. The suspects wanted to plan attacks for "defense of Muslims or retaliation for acts committed against Muslims," authorities have said. They have pleaded not guilty to a July 19, 2006, indictment charging them with providing material support to terrorists and related conspiracy counts. No trial date has been set.
Source: http://www.msnbc.msn.com/id/22655629/

19. *January 14, Tribune-Star* – (Indiana) **Carbon dioxide leak forces evacuation.** Indiana State University's main library was briefly evacuated Monday evening after a student felt nauseated because of a carbon dioxide leak, a university official said. "Just one student felt a little nauseous," an Indiana State University spokesman said. "He got some fresh air and felt better." The student was not taken to a hospital. The evacuation lasted around 15 minutes and the leaking carbon dioxide container was removed from the library.
Source: http://www.tribstar.com/news/local_story_014235446.html

[Return to top]

Emergency Services Sector

20. *January 15, Washington Post* – (National) **Emergency room waits are longer, study finds.** Patients are waiting longer for care in the nation's emergency rooms, a potentially deadly result of the shrinking number of emergency departments and rising demand for services, according to a new study by researchers at Harvard Medical School. Half of all emergency room patients waited 30 minutes or longer before being examined by a

doctor in 2004, a 36 percent increase from a median wait time of 22 minutes in 1997, according to the study, published Monday in the journal Health Affairs. Even those suffering from heart attacks are not guaranteed speedy treatment, with half waiting 20 minutes or longer to be examined in 2004, up from eight minutes in 1997, the study found. The same applies to those with other serious health problems: By 2004, patients whose conditions warranted treatment within 15 minutes were waiting 14 minutes or longer to see a doctor, up from 10 minutes in 1997, the study found. In recent years, several reports have detailed how emergency room care in the United States has been stretched to the breaking point. Between 40 and 50 percent of emergency departments experienced overcrowding in 2004, according to a 2006 study by the federal Centers for Disease Control and Prevention. Three reports issued in 2006 by the Institute of Medicine, a branch of the National Academies, concluded that the U.S. emergency medical system was "overburdened, underfunded, and highly fragmented." Factors include an aging population, shortages of nurses and primary-care doctors, more uninsured patients, more people coming to the emergency room for non-urgent health problems, and the closures of some hospitals as more procedures are done on an outpatient basis, experts say.
Source: http://www.latimes.com/news/nationworld/nation/la-na-emergency15jan15,1,7950892.story?coll=la-headlines-nation

21. *January 15, ScienceDaily* – (National) **Anyone can save a life: National efforts to improve CPR quality underway.** Studies indicate that in many communities only 15 percent to 30 percent of out-of-hospital cardiac arrest victims receive bystander CPR before emergency medical services (EMS) personnel arrive at the scene. Considering that cardiac arrest survival falls an estimated seven percent to 10 percent for every minute without CPR, the low rate of bystander CPR has a big impact on outcomes. A unified effort by the public, educators, and policymakers is needed to reduce deaths from sudden cardiac arrest by increasing the use and effectiveness of cardiopulmonary resuscitation (CPR), according to a new statement from the American Heart Association. The statement, "Reducing barriers for implementation of bystander-initiated cardiopulmonary resuscitation," appears online in Circulation: Journal of the American Heart Association. "Bystander cardiopulmonary resuscitation rates are woefully inadequate, resulting in an enormous missed opportunity to save lives from cardiac arrest," said the statement's lead author. Approximately 166,200 out-of-hospital sudden cardiac arrest deaths occur annually in the United States. Sudden cardiac arrest often results from an irregular heartbeat called ventricular fibrillation (VF) which causes the heart to quiver so that it cannot generate blood flow. Treatment of VF requires CPR to keep blood moving through the body until the patient's heart can be shocked to terminate the VF and allow the heart's pacemaker cells to establish a normal rhythm. In the last decade, automated external defibrillators (AEDs), portable defibrillation machines, have become increasingly common. However, the statement said defibrillation is only one of the four links in the Chain of Survival: (1) early recognition of the emergency and phoning 911 for EMS, (2) early bystander CPR, (3) early delivery of a shock via a defibrillator if indicated, and (4) early advanced life support and post-resuscitation care delivered by healthcare providers. "Quick initiation of CPR, as well as providing high quality CPR, is crucial to survival," said the author. "What's needed is a

two-pronged approach: first, substantially increase the number of bystanders trained in CPR who then provide CPR during an actual emergency and second, improve the quality of training and actual CPR performance through measures of its effectiveness."
Source: http://www.sciencedaily.com/releases/2008/01/080114162509.htm

[Return to top]

Information Technology

22. *January 15, Network World* – (International) **Storm botnet gets profiled at Web site.** Storm, which has grown into a large remotely controlled botnet since the initial worm appeared a year ago to infect victims' machines, is getting a graphic profile on a Web site set up to track it. StormTracker on Secure Computing's TrustedSource.org research portal displays real-time information compiled through sensors maintained in 75 countries. According to the director of intelligence analysis and hosted security at Secure Computing's TrustedSource Labs, Storm has morphed into a botnet capable of various tasks, such as sending spam, establishing malicious Web pages or carrying out phishing attacks. "In the last couple of days, it has conducted phishing attacks against Barclays Bank and the Bank of Nova Scotia," he said. "It's a fast-flux network with thousands of machines around the world, and it's grown so that it's almost impossible to shut down." Secure Computing believes that the Storm botnet is operated by individuals in Russia, based on the firm's analysis and registration of domain names, but would not provide specifics. The Secure Computing representative said the StormTracker site is intended to inform security managers about the botnet's current shape and provide them with information they may wish to use to filter Internet access. The information Secure Computing is compiling is generated dynamically using the firm's Trusted Source Reputation System.
Source: http://www.networkworld.com/news/2008/011508-storm-botnet.html

23. *January 14, IDG News Service* – (International) **10,000 Web sites rigged with advanced hacking attack.** A sophisticated hacking scheme seen early last year is affecting an increasing number of Web servers, including one owned by a major online advertising company, the chief technology officer of Finjan Software said Monday. It appears that a single gang is behind the attacks, since the malicious software it spreads is storing login and password details on one server in Spain, he said. Finjan is trying to get the ISP (Internet service provider) to shut it down, he said. A Web server of an online advertising company that serves 14 million banner ads to other Web sites has also been hacked, he said. That means that the PC of anyone who visits a legitimate site hosting a malicious banner ad could potentially be infected if their computer is not patched, he said. The latest problems show that the power of this particular hacking gang appears to be growing since it was identified early last year. At that time, Finjan said it found a number of Web servers that had been hacked in order to serve malicious code to visitors. The attackers used several methods to hide their tracks and infect a maximum number of PCs. The attack is structured using JavaScript so that the malicious code is only served up once to a PC, which helps avoid repeated tests by security scanning services. Further, hackers also record the IP (Internet Protocol) addresses of crawlers used by search engines and reputation services, which evaluate the risk in visiting certain Web sites.

Those page requests are then served with legitimate content. The JavaScript that starts the exploit also dynamically changes, which makes it more difficult to detect with security software, Finjan said. Once hacked, a Web server hosting hundreds of Web sites will serve up the attack code. The hackers also regularly change the vulnerabilities that the attack looks for in order to increase the chances a computer can become infected, Ben-Itzhak said. After the PC is infected, the malware can start collecting data on the machine, such as documents and passwords. Finjan has dubbed the attack "random js Trojan." Finjan asserts that antivirus software is not as effective since the attack code can change so frequently.
Source: http://www.networkworld.com/news/2008/011408-10000-web-sites-rigged-with.html

24. *January 14, Register* – (National) **Browser vulnerabilities and botnets head threat list.** Security experts have looked into the crystal ball to predict the cyber attacks most likely to cause substantial damage this year. The resulting list drawn together by 12 security experts under the auspices of the SANS Institute, is based on an analysis of emerging attack patterns. Two of the resulting predictions - malware on consumer devices and web application security exploits - have already come true in the early days of 2008, evidence that that the run down is closer to the mark than other security predictions. As is often the case, browser exploits came out as the top threat in the run down, but the risk is evolving. Web site attacks have migrated from simple exploits to more sophisticated attacks based on scripts that cycle through multiple exploits to yet more sophisticated attacks featuring packaged modules. One of the latest such modules, mpack, produces a claimed 10-25 per cent success rate in infecting surfers. Attackers are actively placing exploit code on popular, trusted web sites where users have an expectation of security. Placing better attack tools on trusted sites is giving attackers a huge advantage over the unwary public. Meanwhile attackers have broadened the scope of the vulnerabilities they target to encompass components, such as Flash and QuickTime, that are not automatically patched when the browser is patched. Evolution in existing threats -- including stealthier botnet control techniques and more subtle social engineering approaches in phishing attacks -- is a theme that runs through the whole list. The list includes, for example, increasing sophistication and effectiveness in botnets, cyber espionage efforts by well resourced organizations looking to extract large amounts of data – particularly using targeted phishing, and an increase in mobile phone threats, especially against iPhones and Android-based phones.
Source: http://www.theregister.co.uk/2008/01/14/sans_threat_list/

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

25. *January 14, Associated Press* – (National) **FCC asks Comcast about Internet filter.** Comcast Corp. Monday said it has received letters of inquiry from the Federal Communications Commission regarding complaints that the company actively interferes with its subscribers' Internet traffic. A coalition of consumer groups and legal scholars asked the agency in November to stop Comcast from discriminating against the sharing of certain types of Internet data among subscribers. Two groups also asked the FCC to fine the nation's No. 2 Internet provider $195,000 for every affected subscriber. And Vuze Inc., a company that distributes video using BitTorrent file-sharing technology, later filed a separate complaint, asking the FCC to clarify how much power Internet service providers have in controlling traffic on their lines. In an investigation last year, The Associated Press found that Comcast in some cases hindered file sharing by subscribers who used BitTorrent. The findings, first reported October 19, confirmed claims by users who also noticed interference with other file-sharing applications. Comcast denies it blocks file sharing, but acknowledges milder interventions to improve the flow of traffic for the majority of its customers. "We look forward to responding to the FCC inquiries regarding our broadband network management," said an executive vice president at Comcast, in a statement. "We believe our practices are in accordance with the FCC's policy statement on the Internet where the Commission clearly recognized that reasonable network management is necessary for the good of all customers," he added. Peer-to-peer file sharing is a common way to illegally exchange copyright files, but many businesses also are rushing toward it for legal distribution of video and game content.
Source:
http://news.yahoo.com/s/ap/20080114/ap_on_hi_te/comcast_data_discrimination_2;_ylt=AtEASX3rr7r9C9q36LufvkdH2ocA

26. *January 14, InformationWeek* – (International) **Report critical of cell phone ban on U.S. planes.** While passengers worldwide are allowed to use their mobile phones during flights, the United States remains closed to the idea, consequently causing travelers to be less productive, according to a report released Monday by Freesky Research. The ability to send data and make calls in-flight allows Middle Eastern, Asian, and European business travelers the opportunity to be more productive on commercial airplanes than U.S. travelers, according to the report. The Federal Communications Commission put a rest to the idea of allowing mobile phone use during flights last year. Commercial airlines in the United States continue requiring passengers to turn off their phones before a plane takes off. The FCC is concerned that mobile phones could disrupt other radio communications on planes. But Freesky Research contends that after testing mobile device interference with cockpit communications and navigation equipment for the last five years, and with systems now installed on passenger planes, there is evidence that mobile phones can be used in-flight without harm. **"**As long as the United States maintains its current policy banning cellular antennas from being used on jets, it is allowing other countries to leap ahead with in-flight productivity, while facing mounting evidence that there is no safety benefit to passengers," said the chief analyst at Freesky Research and author of two related reports, in a statement. In Europe, a cellular ground-

based system called OnAir was approved last year for cell phone use in Airbus planes by the European Aviation Safety Agency. Passengers in other countries around the world, including Australia, Turkey, Malaysia, and India, can also use mobile phones during flights, Freesky Research said.
Source:
http://www.informationweek.com/security/showArticle.jhtml;jsessionid=APSY3DKCYVHLAQSNDLPCKH0CJUNN2JVN?articleID=205604708

[Return to top]

Commercial Facilities Sector

27. *January 14, Reuters* – (Arizona) **Trained dogs to help secure U.S. Super Bowl sites.** Dogs trained to detect explosives, especially the kind used by Islamic extremists, will help secure next month's Super Bowl, the biggest event in the U.S. sporting calendar, law authorities said on Monday. An undisclosed number of specially trained Labrador Retrievers have been brought to Phoenix to secure venues for the National Football League's championship game on February 3, the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) said. An ATF agent said the dogs have been taught to recognize explosive materials gathered by the ATF from attacks in Afghanistan, Iraq, Britain, and Spain, such as TATP, or triacetone triperoxide, used by Islamic militants to attack the Madrid and London transport systems in 2004 and 2005.Security for the event is being coordinated with eight federal, state, and local agencies.
Source:
http://news.yahoo.com/s/nm/20080114/us_nm/nfl_superbowl_dc;_ylt=At3A0wFwpitvjXgxsrAbcRwWIr0F

[Return to top]

National Monuments & Icons Sector

28. *January 15, Aspen Times* – (Colorado) **Bark beetle infestation decimates Colorado.** A bark beetle infestation that has already ravaged forests in parts of Colorado grew at an "unprecedented" rate in 2007 and affected 500,000 additional acres, the U.S. Forest Service reported Monday. The growth of the beetle epidemic affecting lodgepole pine forests last year was "unprecedented," said a Rocky Mountain Regional. All mature lodgepole pine forests will be dead in Colorado within three to five years, said a group leader for forest health management in the Rocky Mountain Region. The infestation kills entire hillsides of lodgepole pine trees and leaves behind rust-colored skeletons. Impacts could be as severe as eliminating cover that allows slopes to hold snow and allowing erosion that clouds water quality, officials said.
Source: http://www.aspentimes.com/article/20080115/NEWS/429797840

[Return to top]

Dams Sector

29. *January 15, Post-Tribune* – (Indiana) **Levee breaks turn farmland to lake.** The Kankakee River in Indiana crested Saturday but not before levees along the river had broken in at least two places. More than two dozen farmers battled a break in a levee over the weekend near the Grand Kankakee Marsh Hunt Club, spending 60 hours to fix the 8-foot-deep breach. A drier landscape could take weeks to emerge, and meanwhile the Kankakee River Basin Commission is not sure how much damage the flooding of the Kankakee River has caused to levees and how to pay for repairs.
Source: http://www.post-trib.com/741055,ropflood.article

30. *January 14, Kansas City Star* – (Kansas; Missouri) **Levee-repair delays heighten anxiety of people living near rivers.** In Kansas and Missouri, the U.S. Army Corps of Engineers is beginning work on what is estimated to be $17 million in repairs to levees that were breached or damaged by floods in May and July on the Missouri River and smaller waterways. "It's January now, and there's only one corps project under way," said the chairman of the Missouri Levee and Drainage District Association. "Any way you look at it, it's a slow process. There's got to be a way to improve it." The floods caused enough damage to qualify 38 levees for federal repair dollars. Those include seven breached levees, including a major gap in a Carroll County levee on the Missouri River downstream from Kansas City.
Source: http://www.kansascity.com/news/local/story/444835.html

31. *January 14, WISTV 10 Columbia* – (South Carolina) **Columbia dam gives way, leaving homeowners with eyesore.** In South Carolina, a broken dam has left a Columbia neighborhood with a soggy mess. Neighbors say the dam gave way, causing all the water to rush out of the lake. Since then, there have been complaints of increased respiratory problems and a foul odor coming from the lake bed. They have contacted the Department of Health and Environmental Control and do not know who to contact next. Richland County says they are not responsible for maintenance because it is a private lake. However, they plan to check the problem out and offer recommendations.
Source: http://www.wistv.com/Global/story.asp?S=7623494&nav=0RaP

32. *January 14, Atlanta Journal-Constitution*– (Georgia) **Refilling Gwinnett's Taylor, Richland lakes brings smiles.** Last summer, Gwinnett County, Georgia, drained Taylor and Richland Lakes to give workers better access to the Richland dam, which had to be improved. But months ahead of schedule, work on the Richland dam almost finished and Taylor Lake is just about full. Parched and warm, the past few months have proven advantageous for construction projects, said the head of Gwinnett's department of stormwater management. Crews were able to build construction roads in the bed of dry Richland Lake and reach the dam. To meet state standards, they have replaced packed dirt with concrete. All that remains is to cover the concrete with dirt and sod, so that it looks like a grassy hill. The roads and sedimentation fences will be removed and some landscaping finished. In addition to the Richland Lake dam, county workers had to improve the dam on Channings Lake, which was also drained.
Source:
http://www.ajc.com/metro/content/metro/gwinnett/stories/2008/01/14/lake_gwinnett_0114.html

[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