Department of Homeland Security Daily Open Source Infrastructure Report for 15 January 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- The Associated Press reports that a man blew up a dump truck about a mile away from the Prairie Island nuclear plant in Minnesota. The vice president of the plant site said the plant was put on heightened security for over two hours until officials could determine what had happened. The plant returned to normal activity once investigators determined that the blast was not connected to the plant. (See item 5)
- Vnunet.com reports that security experts have warned of a crimeware attack caused by an "extremely elusive" Trojan that sends data from infected machines direct to the malware author. Stolen data can include documents, passwords, surfing habits or any other sensitive information of interest to the criminal. More than 10,000 websites in the US were infected by this malware in December alone. (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 14, Reuters* – (National) **Oil rises towards $94 as commodities rally.** Oil rose to nearly $94 a barrel on Monday, halting a three-day losing streak amid a wider

commodities rally, as the dollar's weakness and tensions involving Iran countered worries of a global economic downturn. U.S. light crude for February delivery rose $1.04 to $93.73 a barrel by 1315 GMT, off lows of $92.41 earlier in the session. Oil, which hit a record high of $100.09 on January 3, has since mostly fallen on growing fears of a possible economic recession in the United States, which could curb demand in the world's biggest oil consumer. The verbal exchanges between Washington and Tehran have rekindled worries that Iran, the world's fourth-largest crude exporter, could cut oil exports to retaliate against U.S. pressure over its nuclear program. In Nigeria, militants fighting for regional control of the country's oil-producing south detonated a remote-controlled bomb on an oil tanker on Friday, causing a big fire. Analysts said the oil market was caught between the opposing influences of short-term tight supply and downside risks to oil demand from a slowing economy, with geopolitical events and speculators driving prices in the near-term. The Organization of the Petroleum Exporting Countries said on Sunday a slowing global economy would not affect oil demand in the short term and lead to a price collapse.
Source: http://news.yahoo.com/s/nm/20080114/bs_nm/markets_oil_dc_5

2. *January 14, WCVB 5 Boston* – (Massachusetts) **Thousands in dark as Nor'easter moves through.** As of midday on Monday, National Grid reported 15,800 outages, with Foxborough, Stoughton, Easton, Norton, Weymouth and Pembroke being the hardest hit communities in Massachusetts; NSTAR reported 17,000 outages with Walpole being the hardest hit; and Western Massachusetts Electric reported 10,000 outages, mostly in the Springfield area. Crews were working to restore power and hoped all customers would have electricity back by the end of the day.
Source: http://www.thebostonchannel.com/news/15044620/detail.html

[Return to top]

Chemical Industry Sector

3. *January 14, U.S. Environmental Protection Agency* – (South Carolina) **EPA to hold public meeting regarding Columbia Organic Chemical Company site in Columbia, S.C.** The U.S. Environmental Protection Agency (EPA) will hold a public meeting on Thursday, January 17, 2008 regarding the Columbia Organic Chemical Company site in Columbia, South Carolina. EPA and the South Carolina Department of Health and Environmental Control officials will provide information and answer questions about the EPA removal action underway at the site. The facility operated as a specialty chemical facility from 1944 until 1984, at which time the operation was relocated to the Cassatt community in Kershaw County, South Carolina. The site is a three acre property surrounded by a mixture of residential and commercial properties.
Source: http://www.chemicalonline.com/content/news/article.asp?docid=ae90ebfb-8a2e-40b4-82ef-8bcb3d157fe7&atc~c=771+s=773+r=001+l=a&VNETCOOKIE=NO

4. *January 13, WNEP 16 Northeastern and Central Pennsylvania* – (Pennsylvania) **Plant closed after chemical leak.** A chemical plant is closed after a chemical leak Saturday morning forced some Monroe County, Pennsylvania, residents from their homes. Emergency crews were on hand following a chemical leak around 8 a.m. Saturday at

Vertellus Specialties in Delaware Water Gap. A spokesman for Vertellus Specialties Inc. said an employee noticed a plume of vapor and then used the plant's radio system to call other employees and have the plant evacuated. Part of Route 611 was shut down while emergency crews were on scene. Hazmat crews assessed the situation and firefighters evacuated nearby homes just as a precaution. People were allowed to return to their homes Saturday afternoon as clean-up efforts began at the plant. Vertellus makes a chemical to modify food starch and one of the reactants that leaked is flammable. For now, Vertellus Specialties has closed the plant in Delaware Water Gap until the company finds a cause for the spill in the Poconos.
Source: http://www.wnep.com/global/story.asp?s=7615021

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *January 14, Associated Press* – (Minnesota) **Nearby blast puts nuclear plant on temporary high alert.** Workers at the Prairie Island nuclear plant were put on high alert temporarily after a man blew up a dump truck about a mile away. Goodhue County, Minnesota, authorities say a Welch Township man used explosives he had ordered through the mail to blow up the truck on his property Sunday. Workers at the plant heard and felt the blast around 5 p.m. The vice president of the plant site said the plant was put on heightened security from about 5 p.m. to 7:30 p.m. until officials could determine what had happened. He said the plant returned to normal activity once investigators determined that the blast was not connected to the plant.
Source: http://wkbt.com/Global/story.asp?S=7619072

6. *January 13, Associated Press* – (National) **With nuclear rebirth come new worries.** Of the more than 100 nuclear reactors now being built, planned or on order, about half are in China, India and other developing nations. Argentina, Brazil and South Africa plan to expand existing programs; and Vietnam, Thailand, Egypt and Turkey are among the countries considering building their first reactors. The concerns are hardly limited to developing countries. Japan's nuclear power industry has yet to recover from revelations five years ago of dozens of cases of false reporting on the inspections of nuclear reactor cracks. The Swedish operators of a German reactor came under fire last summer for delays in informing the public about a fire at the plant. And a potentially disastrous partial breakdown of a Bulgarian nuclear plant's emergency shutdown mechanism in 2006 went unreported for two months until whistle-blowers made it public. Nuclear transparency will be an even greater problem for countries such as China that have tight government controls on information. The revival, the International Atomic Energy Agency projects, means that nuclear energy could nearly double within two decades to 691 gigawatts — 13.3 percent of all electricity generated. Developing nations insist they are ready for the challenge. But worries persist that bad habits of the past could reflect on nuclear operational safety. Countries with nuclear power are obligated to report all incidents to the IAEA. But a study said most Asian governments vastly underreport industrial accidents to the U.N.'s International Labor Organization — fewer than 1 percent in China's case.
Source:

http://news.yahoo.com/s/ap/20080113/ap_on_sc/nuclear_world;_ylt=AtsUXkQqMKAEWoOWFNi4QNas0NUE

7. *January 13, Patriot-News* – (National) **Tape lit fuse for nuclear changes.** Videotapes of sleeping guards shot by a freshly hired security worker at the Peach Bottom Atomic Power Station in York County, Pennsylvania, are sending ever-widening shock waves through the commercial nuclear community. Since the tapes were made public last year, Exelon Corp., the nation's largest nuclear energy company with 10 plants, including Peach Bottom, Three Mile Island and Limerick in Pennsylvania, announced it would end its contracts with Wackenhut Corp., which employed the guards. The U.S. Nuclear Regulatory Commission, the federal agency responsible for overseeing commercial nuclear plants, launched a review of its procedures and ordered the industry to do the same. The industry is responding, too, creating a task force to examine ways to ensure that staff is fit for duty, said the senior director of operations support for the Nuclear Energy Institute.
Source:
http://www.pennlive.com/news/patriotnews/index.ssf?/base/news/1200192901316190.xml&coll=1

8. *January 12, Asbury Park Press* – (New Jersey) **Oyster Creek plant reports water leak.** The Oyster Creek nuclear power plant in Lacey, New Jersey, reduced power to 67 percent Friday after a water pipe leaked, but the power reduction had no environmental impact, according to plant and state officials. The service water pipe leak is the latest issue the plant has faced recently. It reduced power to 83 percent last month to deal with a small leak in a condenser and, about two weeks later, reduced power to 92 percent because of vibrating turbine control valves. The water pipe began leaking near the plant's water intake structure at about 3 a.m. Friday, said an Oyster Creek spokeswoman. Plant officials reduced power in "a very slow manner in order to mitigate any environmental effects," she said. As of late Friday afternoon, the pipe leak was estimated at about 500 gallons a minute out of a flow of approximately 4,000 gallons a minute. Plant officials were investigating why the pipe began leaking and "are looking at ways that we can repair this on line," said the Oyster Creek spokeswoman.
Source:
http://www.app.com/apps/pbcs.dll/article?AID=/20080112/NEWS03/801120355/1007

[Return to top]

Defense Industrial Base Sector

9. *January 13, Associated Press* – (National) **New boat aims to make SEALs' travels less painful.** An all-composite version of the aluminum Mark V patrol boat is aimed at reducing the wear and tear on boat operators and SEALs by absorbing the impact as the vessel crashes through the waves at 50-plus knots. The goal is a boat that can deliver up to 16 combat-ready Navy SEALS in shape to carry out their missions and will reduce the boat operators' neck, back and joint injuries. "The idea is to build a boat out of the best carbon-Kevlar composite that we can build to reduce those slamming forces," said the president and chief executive officer of Maine Marine Manufacturing LLC. The 82-

foot research prototype unveiled Friday looks similar to current patrol boats, but it has a new hull made from advanced composite materials. Though designed to reduce slamming forces, the prototype is actually 50 percent stronger -- and slightly lighter -- than the aluminum version. Dubbed MAKO for the shark that frequents the Gulf of Maine, the vessel will undergo shipbuilder testing this month in Maine's coastal waters before traveling to Norfolk for further evaluation by the Navy. If it performs as expected, it could be deployed within two to three years.
Source: http://www.cnn.com/2008/TECH/01/13/seals.new.boat.ap/index.html

10. *January 13, Defense Industry Daily* – (National) **Design & preparations continue for the USA's new CVN-21 super-carrier.** As the successor to the 102,000 ton Nimitz Class super-carriers, the CVN-21 program aims to increase aircraft sortie generation rates by 20 percent, increase survivability to better handle future threats, require fewer sailors, and have depot maintenance requirements that could support an increase of up to 25 percent in operational availability. The combination of a new design nuclear propulsion plant and an improved electric plant are expected to provide 2-3 times the electrical generation capacity of previous carriers, which in turn enables systems like an Electromagnetic Aircraft Launching System (replacing steam-driven catapults), Advanced Arresting Gear, and a new integrated warfare system that will leverage advances in open systems architecture. Other CVN-21 features include an enhanced flight deck, improved weapons handling and aircraft servicing efficiency, and a flexible island arrangement allowing for future technology insertion.
Source: http://www.defenseindustrydaily.com/

[Return to top]

Banking and Finance Sector

11. *January 14, WITN 7 Washington* – (National) **Scam targets military spouses.** The American Red Cross is warning military families about a scam that puts a soldier's identity at risk. The group says scam artists are contacting military spouses, saying they work for the "Red Cross." The caller tells the spouse their loved one has been injured in Iraq and has been transported to a hospital in Germany. However, before doctors can treat him, the caller says, they need to complete paperwork. The caller asks for the soldier's social security number and birth date. The American Red Cross says their workers do not directly contact families or dependents of servicemen and women.
Source: http://www.witntv.com/home/headlines/13763802.html

12. *January 14, Marketwire* – (National) **Retailers to encrypt more consumer data in 2008.** "Many retailers have put into place security measures to protect customer credit card numbers to comply with the Payment Card Industry Data Security Standard (PCI DSS)," said nuBridges' vice president of Product Management at the National Retail Federation 97th Annual Convention & EXPO. "In 2008, we'll see more retailers look for ways to protect other consumer information to comply with current state and pending federal breach notification laws." Driving the need to secure personal data beyond credit card numbers is a new marketing strategy aimed at teenagers that employ customer interaction platforms. For example, some retailers ask teens to supply their mobile

phone number so that they can be identified when they walk into a store. Based on their personal buying history, the retailer can then send coupons and specials via the phone to teens as they shop to encourage purchases. In this case, a customer's personal buying history and cell phone number must be protected since retailers have begun accepting payment for merchandise by mobile phones (electronic wallets). Breach notification laws specify what personal identifiable information (PII) must be protected. This information varies from state to state, but can include information such as social security numbers, bank account numbers, birth date, address, phone numbers, passwords and password hints among other data. This creates the need for security solutions that can encrypt data wherever it resides within the store -- at the point of sale terminal, a server or kiosk -- as well as at corporate headquarters and during hardwire and wireless transport.
Source: http://www.marketwire.com/mw/release.do?id=809913

[Return to top]

Transportation Sector

13. *January 14, San Francisco Chronicle* – (California) **Jet backs into another at SFO - no injuries.** A United Airlines Boeing 757 jet that was backing out of a gate at San Francisco International Airport crashed into a SkyWest plane carrying 60 passengers and crew Sunday night in what airport officials called a serious accident. The crash occurred at domestic Terminal 3 as the United plane was being taken out of service and moved without passengers from Gate 80 to a hangar for maintenance. The passengers onboard the SkyWest plane, which was headed to Boise, Idaho, were not injured, said an airport duty manager. The impact caused damage to both planes: Both had part of their tails sheared - specifically the vertical stabilizer assembly - and both had damage to their engines. There were no "wing walkers" on the ground directing the tug as it moved the United plane, said the airport duty manager. There were two individuals on the tug truck, he said. He added that there is no airport policy requiring wing walkers for maintenance moves and that each airline sets it own policy on that matter. A United Airlines spokeswoman said it is the airline's normal procedure not to use wing walkers when taking a plane to the maintenance area. The crash will be investigated by the Federal Aviation Administration, and is certain to raise new questions about safety at the airport.
Source: http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2008/01/14/MN6LUES3S.DTL

14. *January 13, Associated Press* – (Washington) **Abandoned backpack prompts Hood Canal Bridge closure.** The Washington State Patrol closed the Hood Canal Bridge to traffic for more than an hour after a bomb squad was called in to investigate an abandoned backpack. The closure began shortly before 1 p.m. Sunday, after the abandoned bag was found on the bridge between the Olympic and Kitsap peninsulas. Troopers have not said what they found in the backpack.
Source: http://www.kndo.com/Global/story.asp?S=7618120

15. *January 12, Associated Press* – (Georgia) **FAA probes near-collision at Atlanta.** The

Federal Aviation Administration is investigating a near-collision of two airplanes on the runway at Hartsfield-Jackson Atlanta International Airport on Friday. Investigators believe an Atlantic Southeast Airlines flight bound for Greensboro, North Carolina, ignored orders from the control tower to stop its taxi across the runway, coming within seconds of running into a Mexico-bound Delta Air Lines Inc. jet, said a FAA spokeswoman. The ASA pilot acknowledged the orders and repeated them back to controllers in the tower but did not stop, she said. The ASA jet was carrying 44 passengers, and the Delta flight had 130 aboard. Air traffic controllers estimated the planes came within 1,250 feet - or about 2 to 3 seconds - of colliding. Both continued on their scheduled flights and arrived safely at their destinations, airline officials said.
Source: http://apnews.myway.com/article/20080112/D8U46IO00.html

[Return to top]

Postal and Shipping Sector

16. *January 12, KCBD 11 Lubbock* – (Texas) **Slaton man falls sick after opening mail.** The FBI says anthrax was not responsible for a Slaton, Texas, man becoming ill Saturday afternoon after opening his mail, which contained a white, powdery substance. Wolfforth hazmat crews responded to the man's home and delivered the substance to the FBI. The FBI determined the substance was not hazardous, but is still investigating what caused the man to get sick.
Source: http://www.kcbd.com/Global/story.asp?S=7616569&nav=menu69_2_9

[Return to top]

Agriculture and Food Sector

17. *January 14, Los Angeles Times* – (National) **Farmers fear a barnyard Big Brother.** The National Animal Identification System, a federal database of animals to fight disease outbreaks is a threat to privacy and family operations, critics say. The database, which is a Bush administration initiative, is meant to provide a modern tool for tracking disease outbreaks within 48 hours, whether natural or the work of a bioterrorist. Most farm animals, even exotic ones such as llamas, will eventually be registered. Information will be kept on every farm, ranch or stable. And databases will record every animal movement from birth to slaughterhouse, including trips to the vet and county fairs. But the system is spawning a grass-roots revolt. Family farmers see it as an assault on their way of life by a federal bureaucracy with close ties to industrial agriculture. They point out that they will have to track every animal while vast commercial operations will be allowed to track whole herds. Privacy advocates say the database would create an invasive, detailed electronic record of farmers' activities. Religious farming communities, such as the Amish and Mennonites, oppose the system for religious reasons. Within the cattle industry, the database is seen as essential to restore U.S. exports in the international market, which dropped sharply after a Canadian cow infected with mad cow disease was imported to the U.S. in 2003. There are more than 100 million beef cattle and about 10 million dairy cows in the United States. The world's largest beef consumer, the European Union, is sensitive to mad cow disease

because of outbreaks in Britain.
Source: http://www.latimes.com/news/nationworld/nation/la-na-animals14jan14,1,3449562.story?page=2&cset=true&ctrack=1&coll=la-headlines-nation

18. *January 13, Associated Press* – (National) **Meat company recalls beef after 5 illnesses reported in Wisconsin.** Rochester Meat Co. of Rochester, Minnesota, has recalled about 188,000 pounds of ground beef patties and some other products because of E. coli bacteria concerns, after five illnesses were reported in Wisconsin and one in California, the U.S. Agriculture Department's Food Safety and Inspection Service said in a statement Saturday. The affected beef was produced October 30 and November 6. It was shipped to distributors nationwide for use in restaurants and food service institutions. It was not sold by retailers, the USDA service said.
Source: http://www.chicagotribune.com/news/nationworld/chi-ap-mn-beefrecall,1,266010.story

[Return to top]

Water Sector

19. *January 14, Los Angeles Times* – (California) **Water laws may throttle growth.** The planned distribution center for the footwear firm Skechers USA would be one of the largest warehouses in the U.S and would anchor a new community nearby Lake Perris reservoir in California. Now, in a sign of growing water anxieties, the Skechers warehouse and six other large projects in western Riverside County are on hold until March or later because the local water agency could not promise to deliver water to serve them. The dilemma shows what can happen when construction and global trade, key drivers of the regional economy, are reined in by a potential lack of water. The president of the board of directors of the Perris-based Eastern Municipal Water District, one of the largest districts in the state, said that no one on the board wants to hobble the economy, but the restriction is necessary for the time being. He expressed surprise that other water districts have not paused to review their own supplies. The Eastern district may be the first in the region to cite water as the reason for delaying approval of a large project because of the laws. Developers and water officials worry that more agencies may do the same, further weakening a building market already crippled by the sub-prime mortgage crisis.
Source: http://www.latimes.com/news/local/la-me-skechers14jan14,0,3578250,full.story?coll=la-home-center

20. *January 12, News 4 Jacksonville* – (Florida) **North, Central Florida wage water war.** North Florida residents and officials are angered by Central Florida's plans to take millions of gallons of water a day out of the St. Johns and Ocklawaha rivers to meet that area's exploding demand. North Florida officials said that such measures could grave environmental damage, particularly to the north-flowing St. Johns. Jacksonville, St. Johns County, other cities and a river advocacy group said the plan would destroy the delicate balance of saltwater and freshwater needed to preserve critical biological habitat and submerged vegetation. The plan was developed by the St. Johns River Water

Management District after it determined that areas of central Florida could reach their groundwater limits within five years and that by 2025 it will need 200 million gallons of water a day from alternative sources.
Source: http://www.news4jax.com/news/15035990/detail.html

[Return to top]

Public Health and Healthcare Sector

21. *January 14, Napa Valley Times* – (California) **Nasty virus making a mark in Napa.** Local outbreaks of norovirus throughout December and early January are causing headaches for Napa County's public health officials, especially in Napa's retirement communities in California. The Springs of Napa reported 31 cases of the virus between December 31 and January 7, said a public relations specialist for Holiday Retirement, which manages the facility. In response to the outbreak, Springs employees closed down the dining room for approximately 10 days, delivering meals to residents' apartments. The dining area re-opened Friday after no additional cases of the illness were reported. Also, Villa Del Rey, another retirement community in Napa, experienced a possible outbreak of the virus from December 22- 27, 15 of the facility's approximately 80 residents became ill, according to the executive director of the facility. Villa Del Rey had a previous outbreak of norovirus in October 2006, when residents stayed in their apartments for three weeks, she said.
Source:
http://www.napavalleyregister.com/articles/2008/01/14/news/local/iq_4319047.txt

22. *January 13, db Techno* – (International) **Chicken deaths in India, Bangladesh, raise bird flu alerts.** Over the last ten days, thousands of backyard poultry consisting of chickens have all died in India, as well as Bangladesh. Results from tests have shown that they died due to being infected with the bird flu, possibly the H5N1 strain, causing a bird flu alerts in both countries. The chief medical officer in West Bengal, India stated that the preliminary tests, which have been released, have shown that the birds there did die from the bird flu, although it is not clear if it was the H5N1 strain. In Bangladesh, over 500 chickens have been killed at a poultry farm in the northeastern Moulavibazar district area.
Source: http://www.dbtechno.com/health/2008/01/13/chicken-deaths-in-india-bangladesh-raise-bird-flu-alerts/

23. *January 12, Sunday Times* – (International) **Norovirus reaches epidemic levels.** The winter vomiting bug norovirus has struck 2.8 million people in the U.K., with health professionals braced for another rise as people return to schools and offices. The virus is striking down more than 200,000 a week, according to official estimates. Three U.K. hospitals have been placed on red alert, while hundreds of wards up and down the country have been closed to new patients as the number of beds being taken up by bug victims reaches critical levels. The rate of new cases being confirmed has reached the levels of reports during the massive outbreak five years ago, when officials announced an epidemic. Norovirus can prove deadly for vulnerable people, such as children and the elderly. A spokesman for the Health Protection Agency said it was too early to say if the

disease had reached its peak. The Health Protection Agency has confirmed that 1,922 laboratory samples tested positive for norovirus, and, since the virus is often untreated, the agency expects 1,500 cases in the community for every one found in its labs, bringing the total number to 2.8million infected people – or a million new cases each month.
Source: http://www.timesonline.co.uk/tol/news/uk/health/article3176710.ece

Government Facilities Sector

24. *January 13, KEYE TV 42 Austin* – (Texas) **HazMat crews respond to spill at UT; none injured.** Firefighters responded to a chemical spill on the University of Texas campus around 2 p.m. Sunday after a professor working on the fourth floor of Welch Hall discovered a shelf in a storage area had collapsed. About 30 chemicals were spilled on the floor. Firefighters in HazMat gear determined the inert materials posed no threat. There were no injuries.
Source: http://www.keyetv.com/content/news/topnews/story.aspx?content_id=af4de408-1e70-4322-8505-93f4bbb00640

[Return to top]

Emergency Services Sector

25. *January 14, Washington Technology* – (National) **FCC's unanswered questions.** With the Federal Communications Commission's January 24 public auction of radio spectrum approaching, industry representatives are voicing concerns about the planned development of a nationwide public safety wireless broadband network. Interested parties are questioning the viability and oversight of the network and how it will connect with state and local agencies and sellers of similar services. Although many of the issues have been raised before, there is greater urgency as the auction approaches. The auction will sell spectrum made available as broadcasters convert to digital TV. FCC identified bidders last month but declined to specify in which spectrum block they are interested. The D Block includes a 10 MHz segment of 700 MHz bandwidth that FCC set aside for a public safety network. The commission asked participants not to comment publicly to avoid collusion. This is the first time FCC has attempted to construct a national public safety wireless network. The rules call for the winner of the D Block of spectrum to make a section of it available to first responders for voice over IP and data needs on an emergency basis. The spectrum would be governed by a new public/private partnership. In recent weeks, industry executives have expressed uncertainty about the public safety network's creation and operation. The question remains whether the new network can meet public safety needs while earning sufficient profits for commercial operations. Fire and police departments need a robust and extremely reliable network, requiring substantial investment, while commercial users are less demanding and may be served at a lower cost. FCC has touted its plan to establish the nationwide broadband network as a boon for public safety interoperability, allowing radios from different jurisdictions to communicate with one another. At the same time, many states have already started their

own planning for statewide interoperability and it is not clear how the FCC network fits into those plans.
Source: http://www.washingtontechnology.com/print/23_01/32086-1.html

[Return to top]

Information Technology

26. *January 14, vnunet.com* – (National) **Hackers unleash 'insidious' crimeware attack.** Security experts have warned of a crimeware attack that threatens to turn highly trusted websites into "insidious traps" for unwary visitors. Finjan's Malicious Code Research Center said that more than 10,000 websites in the US were infected by this malware in December alone. The attack, which the firm has designated 'random js toolkit,' is an "extremely elusive" Trojan that sends data from infected machines direct to the malware author. Stolen data can include documents, passwords, surfing habits or any other sensitive information of interest to the criminal. The JavaScript toolkit is created dynamically and changes every time it is accessed. This makes it almost impossible for traditional signature-based anti-malware products to detect. Finjan's chief technology officer explained that signature-based detection for dynamic script is ineffective. "'Signaturing' the exploiting code itself is not effective, since these exploits change continually to stay ahead of current zero-day threats and available patches," he said. "Keeping an up-to-date list of 'highly-trusted/doubtful' domains serves only as a limited defense against this attack vector." He added that the 'random js toolkit' is an example of the recent trend among cyber-criminals to undermine 'trusted' websites. "Studies in mid-2007 showed nearly 30,000 infected web pages being created every day," he said. "About 80 per cent of pages hosting malicious software or containing drive-by downloads with damaging content were located on hacked legitimate sites. Today the situation is much worse."
Source: http://www.vnunet.com/vnunet/news/2207136/hackers-unleash-insidious

27. *January 13, IDG News Service* – (National) **New Rootkit uses old trick to hide.** A new type of malicious software has emerged, using a decades-old technique to hide itself from antivirus software. The malware, called Trojan.Mebroot by Symantec, installs itself on the first part of the computer's hard drive to be read on startup, then makes changes to the Windows kernel, making it hard for security software to detect it. Criminals have been installing Trojan.Mebroot, known as a master boot record rootkit, since mid-December, and were able to infect nearly 5,000 users in two separate attacks. Once installed, the malware gives attackers control over the victim's machine. The criminals are using several different versions of this attack code, some of which are not currently being detected by some antivirus products.
Source:
http://news.yahoo.com/s/pcworld/20080113/tc_pcworld/141300;_ylt=AhNWUvRfMyeRwsrJ8rjf3t6DzdAF

28. *January 12, IDG News Service* – (National) **Hacked MySpace page serves up fake Windows update.** There is now one more reason to be security-conscious while using MySpace.com: fake Microsoft updates. Using a hacked MySpace profile, online

criminals are trying to trick victims into downloading a malicious Trojan Horse program by disguising it as a Microsoft update, according to researchers at security vendor McAfee. The attack is certainly not widespread -- McAfee has seen it used on only one MySpace profile -- but it does show how sites like MySpace can be abused by criminals. Web surfers are presented with what appears to be a popup window advising them to download the latest version of Microsoft's Windows Malicious Software Removal Tool, which was just released this Tuesday. This software is distributed by Microsoft to help Windows users rid their systems of malware. In reality, the popup window is just part of a larger image that takes up most of the computer screen. If the user clicks anywhere on this image, his computer will then begin to download the Trojan program. The Trojan, known as TFactory, is a well-known piece of code that has been used by criminals for well over a year, according to a security research manager with McAfee. Hackers were able to launch this attack because they either discovered a flaw in the MySpace code or found a way of taking over user accounts, he said. "Our best guess is [the owner of the one MySpace profile] just got their password and user name phished," he said. Social networking sites allow their members to use an array of powerful Web programming tools that are increasingly coming under the scrutiny of hackers looking for ways to misuse them. In November, hackers found a way to serve up Web-based attack code from the MySpace profiles of a number of popular musical artists.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9057078&taxonomyId=17&intsrc=kc_top

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

29. *January 13, Baltimore Sun* – (National) **FCC warns of fraud via phone relay service.** The Federal Communications Commission is warning businesses that people posing as hearing-impaired consumers have been misusing the Internet-based telecommunications relay service (TRS) to commit fraudulent business transactions. The Americans with Disabilities Act of 1990 and FCC regulations require that calls made using TRS be "functionally equivalent" to telephone calls. Reaching a specially trained communications assistant on TRS and instructing them to make a call is, in effect, the same as receiving a dial tone. Anyone can use TRS, and unfortunately, the FCC says, people without disabilities who are posing as hearing-impaired are using TRS and stolen or fake credit cards to scam businesses. While the ADA prohibits businesses from rejecting calls made using TRS, businesses can take steps to protect themselves against fraud. The FCC is working with the Department of Justice, FBI and Federal Trade

Commission to stop fraudulent transactions made by phone or over the Internet. To better protect yourself, the FCC urges merchants accepting orders by telephone for goods or services to take steps to ensure that any order placed by phone is valid and the purchaser is authorized to use a particular credit card. Merchants should also beware of callers who are happy to order "whatever you have in stock; supply multiple credit cards as one or more are declined; can't provide the credit card verification code number (the three-digit number on the back of the card); want goods shipped through a third party and/or to an overseas location; and change delivery or payment method after the order has been approved." If you believe you have been a victim of fraud or attempted fraud, report it to the FTC at www.ftc.gov or 888-FTC HELP.
Source: http://www.baltimoresun.com/business/bal-bz.ml.scam13jan13,0,2315581.story

[Return to top]

Commercial Facilities Sector

Nothing to report.

[Return to top]

National Monuments & Icons Sector

Nothing to report.

[Return to top]

Dams Sector

30. *January 12, Associated Press* – (Maine) **Plan to remove Fort Halifax dam found complete.** The town of Winslow's planning board says FPL Energy's proposal to partially remove the Fort Halifax Dam in order to allow sea-run fish to swim farther upstream is complete. The ruling does not mean the project is approved. The town has opposed breaching the dam since it surfaced five years ago. In August, the Maine Supreme Court denied an appeal by a group of residents who wanted to block the project. The removal of a dam downstream in Augusta in 1999 allowed the upstream migration of sea-run fish, including sturgeon and striped bass, to Waterville for the first time in more than a century and a half.
Source: http://www.boston.com/news/local/maine/articles/2008/01/12/plan_to_remove_fort_halifax_dam_found_complete/

31. *January 12, Associated Press* – (Louisiana) **Corps: More clay needed for levee work.** The greatest obstacle the Army Corps of Engineers faces in raising the region's levees is a lack of clay, an official says. The deputy commander and deputy district engineer of the New Orleans District, said sufficient dirt or clay is "absolutely critical to get this mission accomplished." The corps plans to raise more than 200 miles of levees over the next few years to bring southeast Louisiana's levee system to a 100-year level of

protection. To do that, the corps says it needs 100 million cubic yards of clay, enough to fill the Superdome about 20 times. So far, it has found less than one-third of that.
Source: http://www.nola.com/newsflash/index.ssf?/base/news-36/12001760526560.xml&storylist=louisiana

32. *January 12, Associated Press* – (Indiana) **False report spurs dam fears.** Hours after torrential rain pushed the Tippecanoe River out of its banks earlier this week, the White County Emergency Management office was bombarded by calls from panicked callers who thought a nearby hydroelectric dam had failed. As it turned out, the Norway Dam just north of Monticello was in no danger of a breach. The unfounded fears arose from an inaccurate National Weather Service flash-flood statement that said that the dam's failure "is becoming more likely." Within two hours, the weather service corrected its warning to remove that wording. The confusion over the dam follows concern over the condition of Indiana's 1,100 state-regulated dams, many of which need significant repairs or upgrades. A 2004 report card on the nation's dams by the American Society of Civil Engineers put the estimated cost of upgrading Indiana's most deficient dams at $199.2 million. An analysis of state records in 2005 by The Journal Gazette and Fort Wayne television station WPTA found that half of Indiana's state-owned dams needed significant repairs -- even as the state Department of Natural Resources was pressing private-dam owners to make safety improvements. The assistant director of the department's water division said the state has spent millions of dollars on repairs and rehabilitation of state-owned dams over the last several years. Aside from Indiana's approximately 75 state-owned dams in its parks and recreation areas, a handful -- such as the Norway Dam -- are utility-owned. But most of the state's 1,100 dams are relatively small earthen structures built by private landowners to form lakes for recreation, create water supplies or control flooding.
Source: http://www.courier-journal.com/apps/pbcs.dll/article?AID=/20080112/NEWS02/801120462

[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