Department of Homeland Security Daily Open Source Infrastructure Report for 22 January 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- The According to Network World and other sources, the Federal Energy Regulatory Commission Friday approved eight "critical infrastructure protection" standards intended to protect the electric-power grid operated by the nation's utilities from coming under cyberattack. The final, complete text of FERC's regulatory order is expected out in the next few days, and the commission did indicate it expected the energy industry to improve its power-control systems, if need be, to meet the new security guidelines, in spite of previously voiced concerns. (See item **2**)
- CBS News reported that the FAA called an emergency meeting after another near mid-air collision at New Jersey's Newark Liberty Airport Wednesday, the second near miss in two months. The FAA is investigating the incident and the possibility that a "procedural error" caused a temporary loss of communication with one of two Continental Airlines flights that at one point came within 600 feet of each other. (See item **13**)

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 19, Washington Post* – (International) **Hackers have attacked foreign utilities, CIA analyst says.** In a rare public warning to the power and utility industry, a CIA

analyst this week said cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities. The remarks come as cyber attackers have made increasingly sophisticated intrusions into corporate computer systems, costing companies worldwide more than $20 billion each year, according to some estimates. Over the past year to 18 months, there has been "a huge increase in focused attacks on our national infrastructure networks. The U.S. electricity grid has always been vulnerable to outages. "Cybersecurity is a different kind of threat, however," the commission's chairman, said in a statement this week. "This threat is a conscious threat posed by a single hacker, or even an organized group that may be deliberately trying to disrupt the grid."
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/01/18/AR2008011803277.html?hpid=moreheadlines

2. *January 17, Network World* – (National) **Group defines cyberattack prevention rules for nation's power grid.** The Washington-based Federal Energy Regulatory Commission Friday approved eight "critical infrastructure protection" (CIP) standards intended to protect the electric-power grid operated by the nation's utilities from coming under cyberattack because of poor access control, software vulnerabilities or other weaknesses in their data-control systems. FERC's chairman called the commission's decision a milestone in "adopting the first mandatory and enforceable reliability standards that address cybersecurity concerns on the bulk power system in the United States." The CIP standards were proposed by the North American Electric Reliability Corporation (NERC), which FERC has designated as the organization that will oversee compliance with them. While the final, complete text of FERC's regulatory order has not yet been issued – it is expected out in the next few days -- the commission did indicate it expected the energy industry to improve its power-control systems, if need be, to meet the new security guidelines, in spite of concerns voiced that the older system-control and data-acquisition (SCADA) systems running power grids can not be upgraded to meet the security requirements.
Source: http://www.networkworld.com/news/2008/011708-ferc-power-grid-reliability-standards.html?page=1

3. *January 17, Fox News* – (Utah) **Report: Owners of collapsed Utah mine knew of structural problems.** The owners of the Utah coal mine, where nine miners were killed in a cave-in and subsequent rescue effort, knew in the months leading up to the disaster that the mine had serious structural problems, according to a report in the Salt Lake Tribune on Thursday. According to documents obtained by the Tribune, a mine co-owner knew of a severe bounce on March 10 that forced the evacuation of miners and equipment. According to the Tribune report, mine operations moved farther south from the area of the March bounce. The miners killed in the August collapse were working in an area about 900 feet away from the site of the March incident when the mine collapsed. According to the Tribune report, the March incident was never officially reported to federal regulators, as required by law.
Source: http://www.foxnews.com/story/0,2933,323686,00.html

4. *January 17, News & Observer* – (North Carolina) **Activists campaign against Cliffside**

plant. The N.C. Waste Awareness and Reduction Network, a Durham organization, is placing newspaper ads statewide and plans to engage in civil disobedience in a bid to block Duke Energy's proposed coal-burning plant near Charlotte, North Carolina. Activists are organizing rallies to draw public attention to the perils of environmental damage caused by major power plants. The ads urged the public to ask Duke Energy's chief executive to pull the plug on the power plant and to encourage North Carolina's governor to oppose the plant. Plans for several dozen coal-burning plants in the nation have been withdrawn or delayed in recent years amid growing fears of global warming, emboldening activists to try to add Cliffside to the list of cancellations.
Source: http://www.charlotte.com/business/breaking_news/story/450800.html

5. *January 17, Reuters* – (Texas) **Safety board says to probe BP Texas refinery death.** The U.S. Chemical Safety Board said on Thursday it was sending investigators to probe the latest death at BP Plc.'s giant Texas refinery. A supervisor at the Texas City, Texas, refinery was killed on Monday when a lid blew off a giant water filtration unit as it was being restarted. He was the third worker killed at the plant since a 2005 explosion killed 15 workers. "BP officials today informed the Board that a chemical explosion may have been involved in the overpressure event leading to the death of the employee," the CSB said. "Earlier reports had suggested that water pressure was responsible." The CSB has jurisdiction to investigate industrial chemical accidents and make recommendations for improvements in safety. The board cannot issue regulations or penalties.
Source: http://news.yahoo.com/s/nm/20080118/us_nm/bp_texascity_dc;_ylt=AqlfeyZe6MUBoRkpUPqVyO0WIr0F

[Return to top]

Chemical Industry Sector

6. *January 18, San Mateo Daily Journal* – (California) **Hazmat snafu sparks concern; probe in works.** On Tuesday, four containers of highly concentrated chlorine were spotted in San Mateo, California. Two of the unmarked containers leaked their contents onto the street, forcing a complete closure of the area until the hazardous materials team could neutralize and dispose of the chlorine. The street closure caused traffic backups into downtown. The chlorine had a 12.5 concentration, more than 10 times what would be used in the average pool. It is used to digest organic waste and it cannot be washed down a storm drain, said the district coordinator for the San Mateo County Office of Emergency Services. The hazmat team neutralized the chlorine with citric acid. However, it initially did not have enough on hand and the team was forced to wait until additional citric acid was located, he added. Officials say the spill could have been cleaned up more quickly and are looking into ways to prevent another time-consuming traffic backup.
Source: http://www.smdailyjournal.com/article_preview.php?id=86095

7. *January 17, Associated Press* – (Washington) **Tacoma chemical plant to pay nearly $75,000 for chlorine leak.** A bleach plant on the Tacoma Tideflats agreed to pay $75,000 for being tardy in reporting a chlorine leak that sent about 25 people to

hospitals. Under the deal announced yesterday by the Environmental Protection Agency, Olin Chlor Alkali Products, agreed to pay a $16,000 penalty and to donate $69,000 worth of emergency equipment to the Tacoma Fire Department. Nearly 900 pounds of chlorine was released in February as a worker was loading a tank. The chemical turns into a gas in the air. None of the firefighters or others who were checked at hospitals had to be admitted.
Source: http://seattlepi.nwsource.com/local/6420ap_wa_chlorine_penalty.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

8. *January 17, Associated Press* – (Kansas) **Nuclear plant comes back online.** The Wolf Creek nuclear power plant in southeast Kansas has gone back online after issues with the safety system were resolved. The plant resumed supplying energy to the power grid after being shut down since last Friday. A spokeswoman for Wolf Creek said the problems included a system of pipes that normally carry water in the event of an emergency. Last Friday, operators discovered the pipes had pockets of air and gas, which have since been reduced to acceptable limits.
Source: http://www.nebraska.tv/Global/story.asp?S=7736084

9. *January 17, United Press International* – (Tennessee) **Nuclear reactor shut down.** A spokesman for the Sequoyah Nuclear Plant in Soddy-Daisy, Tennessee, said the Unit 1 reactor was manually shut down after a water valve closed unexpectedly. A spokesman for the Tennessee Valley Authority, which operates the plant, said a valve that regulates water flow into a steam generator unexpectedly closed Wednesday, leading operators to manually shut down the unit, the Knoxville News Sentinel reported Thursday. The valve that closed was designed to control feedwater flow into the steam generator.
Source: http://www.tradingmarkets.com/.site/news/Stock%20News/1001945/

[Return to top]

Defense Industrial Base Sector

10. *January 17, RTT News* – (National) **Rome Research receives $25.6 million Navy contract award.** Rome Research announced that it has received a $25.6 million contract award from the U.S. Navy to operate and maintain communications facilities supporting the United States Naval Computer & Telecommunications Station Guam. The company noted that, as per the contract, it would offer around-the-clock technical services in support of Naval Radio Telecommunications Facility and U.S. Air Force Scope Command radio station in Barrigada, Guam, and the Satellite Communications Facility and Technical Control Facility in Finegayan, Guam.
Source: http://www.tradingmarkets.com/.site/news/BREAKING%20NEWS/998912/

[Return to top]

Banking and Finance Sector

11. *January 18, Bellingham Herald* – (National) **FBI warns of e-mail scam.** The FBI is warning people not to respond to an e-mail scam that uses the FBI's seal, letterhead, banner, and/or picture of its director to intimidate people into giving up personal information. The e-mail might claim to be a lottery endorsement or inheritance notification. Using the FBI's name may convince some people the e-mail is legitimate, but people should not respond, according to an FBI press release. The FBI does not send out emails asking for personal information from citizens, the press release said.
Source: http://www.bellinghamherald.com/102/story/294679.html

12. *January 17, Associated Press* – (National) **Personal information lost on 650,000 credit card holders after computer tape goes missing.** Personal information on about 650,000 customers of J.C. Penney and up to 100 other retailers could be compromised after a computer tape went missing. GE Money, which handles credit card operations for Penney and many other retailers, said Thursday night that the missing information includes Social Security numbers for about 150,000 people. The information was on a backup computer tape that was discovered missing last October. It was being stored at a warehouse run by Iron Mountain Inc., a data storage company, and was never checked out, but cannot be found either, said a spokesman for GE Money, part of General Electric Capital Corp. He said there was "no indication of theft or anything of that sort," and no evidence of fraudulent activity on the accounts involved. An Iron Mountain spokesman said it would take specialized skills for someone to glean the personal data from the tape. The spokesman for GE Money declined to identify the other retailers whose customers' information is missing but said "it includes many of the large retail organizations." He said GE Money was paying for 12 months of credit-monitoring service for customers whose Social Security numbers were on the tape.
Source: http://www.foxnews.com/story/0,2933,323712,00.html

[Return to top]

Transportation Sector

13. *January 18, CBS* – (New Jersey) **Another near collision rattles Newark Liberty.** There was another near mid-air collision at New Jersey's Newark Liberty Airport Wednesday, forcing the Federal Aviation Administration to call an emergency meeting on the matter. For the second time in two months, two planes barely missed each other in the sky. This morning, officials are trying to determine what is happening at the airport. The FAA is stepping in to investigate and try to get to the bottom of it so it does not happen again. As the planes, a Continental Flight from Phoenix, Arizona, and Continental Express Flight from Halifax, Nova Scotia, came in for landings on Wednesday, the space between them became very narrow, narrow to the point that there was only 600 feet between the two. Investigators blame an air traffic controller at TRACON -- Terminal Radar Approach on Long Island -- who was supposed to give the Continental Express crew the tower frequency for Newark, but instead guided the crew to the wrong frequency, the one for Teterboro Airport 13 miles away. The FAA is

expected to hold an emergency meeting on this so called 'procedural error' later on Friday.
Source: http://wcbstv.com/local/newark.airport.continental.2.632715.html

14. *January 18, Associated Press* – (New York; New Jersey) **Officials question departure system switch at LI airport.** Long Island MacArthur Airport is losing a computer system for okaying flight departures, forcing air traffic controllers to make phone calls to clear each plane and prompting concerns about delays. The Departure Spacing Program will be shifted "soon" to Morristown Municipal Airport in Morristown, New Jersey, a Federal Aviation Administration spokeswoman said. She said the change would not cause backlogs at MacArthur, a growing facility that handles nearly 100 flights per day, according to its operator, the Islip Town government. MacArthur air traffic controllers and some elected officials disagree. They say making phone calls - instead of using a system that automatically assesses air traffic conditions, calculates the most efficient routes and approves flights for takeoff - cannot help but cause delays. The system was installed at in 2002 at MacArthur, which is about 50 miles from Manhattan. More than 2.1 million passengers used the airport in 2005, the last year for which figures were immediately available early Friday.
Source: http://www.newsday.com/news/local/wire/newyork/ny-bc-ny--macarthurairport0118jan18,0,5473053.story

15. *January 18, Chattanooga Times Free Press* – (Tennessee; Alabama; Georgia) **Bridges in Tennessee, other states get another look.** Tennessee, Georgia, and Alabama officials again are looking at the design and strength of bridges similar to the Minneapolis truss bridge that fell August 1, 2007. The chairman of the National Transportation Safety Board on Tuesday said the agency's investigation of that bridge collapse found that the steel gusset plates connecting the bridge's support beams were only half as thick as they should have been. That undersizing was a critical factor in the collapse, he said, and state inspectors should check similar bridges for such design flaws and stress capacity. In Tennessee, there are about 60 truss bridges that make use of gusset plates and are similar to the Minneapolis bridge. Georgia officials, too, said they feel confident they are meeting the new recommendations. In Georgia, there are up to 35 highway deck truss bridges with steel gussets, state transportation officials said in August. Alabama Department of Transportation officials began Thursday to re-inspect their state's three bridges that are most like the one in Minneapolis, according to the Associated Press.
Source: http://www.timesfreepress.com/absolutenm/templates/local.aspx?articleid=28552&zoneid=77

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture and Food Sector

16. *January 18, Boston Globe* – (Massachusetts) **Fatal germ found on production line at dairy.** A germ that killed three people and sickened two others originated on the production line of a mom-and-pop dairy in Shrewsbury, Massachusetts, state disease investigators reported yesterday as they provided the clearest evidence yet of how milk became contaminated with the lethal bacteria. Tests performed on the Whittier Farms plant found a strain of listeria on the floor that was identical to the type found in people who became ill last year after drinking the dairy's milk. Investigators discovered the germ near a key piece of equipment used after milk is pasteurized. That same strain was also identified in seven unopened containers of milk the state removed from a retail store adjacent to the Whittier Farms production facility. The germ was found in skim milk as well as coffee-, chocolate-, vanilla-, and strawberry-flavored milk. The review of the Whittier production line also discovered unrelated strains of listeria in a drain, an unwashed bottle, and another piece of equipment. State investigators said they were unsure how listeria made its way inside the Whittier plant, which had received good marks in earlier inspection reports.
    Source:
    http://www.boston.com/news/local/articles/2008/01/18/fatal_germ_found_on_production_line_at_dairy/

[Return to top]

Water Sector

17. *January 17, Reuters* – (West Virginia) **Massey settles EPA water lawsuit for $20 million.** Massey Energy Co. said on Thursday that it would pay $20 million to settle a lawsuit with the U.S. Environmental Protection Agency over claims that it violated the Clean Water Act at its coal mines. According to the EPA lawsuit filed by in federal court in West Virginia in May, the company discharged pollutants in excess of its permit limits about 4,100 times from January 2000 through March 2006. Massey disputed those claims. The EPA said that in addition to the penalty, Massey will invest about $10 million to develop and implement a set of procedures to prevent future violations. It said Massey had agreed to take measures at all of its facilities that will prevent about 380 million pounds of sediment and other pollutants from entering U.S. waters each year. In addition to the settlement, the company agreed to perform 20 water quality improvement projects on the Little Coal River in West Virginia and to set aside 200 acres of riverfront property for conservation.
    Source: http://www.reuters.com/article/environmentNews/idUSWNAS679920080118

[Return to top]

Public Health and Healthcare Sector

18. *January 18, Xinhua* – (International) **Bird flu breaks out in southern Ukraine.** A new outbreak of bird flu was detected in the village of Rifne on the Crimean peninsula in

southern Ukraine this week, the country's Emergency Situations Ministry said in a statement Friday. The outbreak is in same region that was struck in late 2005. A total of 153 birds died suddenly, January 15-17, at a private farm where more than 25,000 poultry birds were kept, the statement said. DNA of the H5N1 virus was found by tests conducted late Thursday. "The village has been sealed off, and guards have been posted at entry points and a quarantine is in place. All the birds are being incinerated," the ministry said.
Source: http://news.xinhuanet.com/english/2008-01/18/content_7449275.htm

19. *January 18, Agence France-Presse* – (International) **Iran detects new bird flu outbreak.** Iranian veterinary authorities have detected a new outbreak of the deadly H5N1 bird flu virus among migratory swans and indigenous ducks and geese in Anzali and Barzanghib, in the north of the country, the ISNA news agency reported on Friday. "All the chickens in the neighboring village have been destroyed," a veterinary official said, adding that no cases of bird flu had been found among farm birds.
Source: http://afp.google.com/article/ALeqM5jqs_WMu7sObzkdDXfBzTw5DFrTxA

20. *January 17, Agence France-Presse* – (National) **New virus linked to rare but lethal skin cancer.** U.S. researchers have discovered a new virus they believe may be linked to a rare but extremely lethal type of skin cancer, a study released Thursday said. Merkel cell carcinoma mostly afflicts the elderly and people with weaker immune systems, including AIDS and transplant patients. In a study published in the journal Science, a research team from the University of Pittsburgh Cancer Institute said it found a strong link between the rare cancer and a new virus they called Merkel cell polyomavirus (MCV). "This is the first polyomavirus to be strongly associated with a particular type of human tumor," said a member of the research team. While the researchers emphasized that more study was needed to confirm the link, they said the discovery could lead to new cancer treatments.
Source: http://afp.google.com/article/ALeqM5iZkhXLdR0R7IigPHbK8wSiP-Adgg

Government Facilities Sector

21. *January 18, WUSA 9 Washington, DC* – (District of Columbia) **Capitol Hill police arrest armed man.** Capitol Police arrested an armed man Friday afternoon. The man was walking down 1st Street NE with a tactical vest, a loaded shotgun, a tactical bow and arrow, and a samurai sword in a hidden case behind his back. His Chevy with Utah license plates came up positive for explosive traces when the dogs sniffed it. There are more weapons in the car. The area has been cordoned off during the investigation.
Source: http://www.wusa9.com/news/local/story.aspx?storyid=67470

22. *January 17, Inside Bay Area* – (California) **County Administration Building evacuated due to bomb scare.** A bomb scare forced the evacuation of employees at the Alameda County Administration Building Thursday afternoon for nearly two hours before authorities searched the building and determined the threat was unfounded. A spokesman for the Sherriff said he did not know any details about the bomb threat, such

as whether it was phoned in.
Source: http://www.insidebayarea.com/localnews/ci_8004017

23. *January 17, Thomson Financial*– (District of Columbia) **World Bank receives bomb threat, closes buildings.** The World Bank said it had received a telephoned bomb threat and was closing all its office buildings in Washington, DC. "World Bank Group Corporate Security is investigating a bomb threat received by telephone. The Bank is working with law enforcement officials to determine the validity of the threat," the Bank said in an online statement. The Bank said it was closing all its leased and owned buildings in Washington on Friday "as a precautionary measure."
Source: http://www.forbes.com/afxnewslimited/feeds/afx/2008/01/18/afx4548263.html

[Return to top]

Emergency Services Sector

24. *January 17, Island Packet* – (South Carolina) **Massive emergency drill to take place in South Carolina.** The scene: An earthquake measuring 7.3 on the Richter scale strikes Beaufort County. In the chaotic aftermath as National Guard troops rush in to assist local emergency officials, terrorists attack local military bases or key infrastructure. County staffers will react to over the course of three days beginning April 21. The county is one of two places in the U.S. participating in the National Guard exercise called "Vigilant Guard." The simulation is estimated to bring 2,000 people, more than 200 vehicles, and millions of dollars to the county during the exercise. The simulation will be divided into 50 missions spread across the county. Over the three days, local officials, with the help of guardsmen and state and federal crews will: conduct search and rescue simulations, in Bluffton, create a mobile medical hospital on Hilton Head Island, evacuate by air 150 "quake victims" from Hilton Head, and distribute goods to southern and northern Beaufort County.
Source: http://www.emsresponder.com/web/online/Top-EMS-News/Massive-Emergency-Drill-to-Take-Place-in-South-Carolina-/1$6863

[Return to top]

Information Technology

25. *January 18, Computerworld* – (International) **Skype plugs critical bug with temp move.** Hackers can exploit newly uncovered vulnerabilities in Skype Ltd.'s popular chat and VoIP software to overtake a Windows PC, security researchers said Thursday. By Friday morning, Skype had confirmed one of the bugs, slapped the highest-possible vulnerability rating on it and temporarily disabled the feature used to exploit the flaw. Early on Thursday, a noted Israeli researcher had spelled out what he called a "cross-zone scripting vulnerability" in Skype that could be leveraged by attackers armed with malicious video files. The way in, he explained, was through a security door that Skype left wide open. "Skype uses [Microsoft Corp.'s] Internet Explorer Web control to render internal and external HTML pages," he said Thursday. If an attacker manages to inject a malicious script into any of those HTML pages, he can completely compromise the

machine. In a demonstration, he posted a video file to the Dailymotion video-sharing service that, when called using the software's Add Video to Chat feature, runs harmless arbitrary code. The exploit relied on a separate cross-site scripting vulnerability on Dailymotion, which is one of Skype's video partners. The innocuous demo, however, could be replaced by attack code of the hacker's choice. "An attacker can now upload a movie, set a kewl popular keyword, and own any user that will search for a video with those keywords through Skype," he noted. Early Friday, Skype posted a security advisory that acknowledged the cross-zone scripting bug, saying that it affected all Windows versions of the software, including 3.5 and the most-up-to-date 3.6. Skype also pegged the flaw as a "10" in the Common Vulnerability Scoring System, the highest rating allowed by the security industry's standard bug ranking system. Skype does not yet have a patch in place; so instead, it simply shut off access to Dailymotion. "Skype has temporarily disabled users' ability to add videos from Dailymotion gallery until an official fix has been made available," the security bulletin said.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9057778&source=rss_topic17

26. *January 17, IDG News Service* – (National) **Attack code released for critical Windows flaw.** In what may be the first step toward a major security problem, security researchers have released attack code that will crash Windows machines that are susceptible to a recently patched bug in the operating system. The code is not available to the general public. It was released Thursday to security professionals who use Immunity's Canvas computer security testing software. It causes the Windows system to crash, but does not let the attacker run malicious software on the victim's system. "It reliably crashes Windows machines," said Immunity's chief technology officer. "In fact, it blue-screened our print server by accident -- this is a broadcast attack, after all." That is the biggest concern for security experts who worry that a more dangerous attack may soon follow as researchers dig further into the vulnerability. The bug is particularly troublesome for two reasons. First, it affects a widely used Windows component that is turned on by default. Worse, no user interaction is required to trigger the flaw, meaning that it could be exploited in a self-copying worm attack. Microsoft patched the flaw in its MS08-001 update, released last week, but it takes time for enterprise users to test and install Microsoft's patches. The flaw lies in the way Windows processes networking traffic that uses IGMP (Internet Group Management Protocol) and the MLD (Multicast Listener Discovery) protocol, which are used to send data to many systems at the same time. The protocols are used by a range of applications including messaging, Web conferencing and software distribution products.
Source: http://www.networkworld.com/news/2008/011708-attack-code-released-for-critical.html

27. *January 17, InformationWeek* – (National) **Yahoo's CAPTCHA security reportedly broken.** Yahoo may soon see a surge in spam coming from Yahoo Mail accounts. "John Wane," who identifies himself as a Russian security researcher, has posted software that he claims can defeat the CAPTCHA system Yahoo uses to prevent automated registration of free Yahoo Mail accounts. CAPTCHA stands for Completely Automated

Public Turing test to tell Computers and Humans Apart. It is a technique that presents an image depicting distorted text that people, but not machines, can identify. Large e-mail service providers like Google, Microsoft, and Yahoo present CAPTCHA images to users signing up for new accounts to make sure that there is a real person behind the registration information. These companies do so to discourage spammers from using automated methods to register thousands of free online accounts to send spam. CAPTCHAs are also used to prevent spam in blogs and other online forums, automated ballot stuffing for online polls, and automated password guessing attacks. "Few months ago, we received information that [a] Yahoo CAPTCHA recognition system exists in the wild with the recognition rate about 30%," Wane says in a blog post. "So we decided to conduct few experiments. We explored Yahoo CAPTCHA and designed a similar system with even better recognition rate (about 35%)." Various automated methods exist to defeat CAPTCHA schemes, but the CAPTCHAs used by Google, Microsoft, and Yahoo have remained difficult for computers to crack. If the software works as advertised, and it is not clear that it does, it could force Yahoo and other companies to spend yet more money to defend against spammers.
Source:
http://www.informationweek.com/management/showArticle.jhtml;jsessionid=OABRKDXIVXPNAQSNDLPSKH0CJUNN2JVN?articleID=205900620

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

28. *January 18, RCR Wireless News* – (National) **National Research Council calls for further studies on cellphone radiation.** A National Research Council report calls for more research into the potential health effects of long-term exposure to radiation emitted by cellphones and other wireless devices, with U.S. scientists anxious to gather more data on any risks posed to children, pregnant women and fetuses by handsets as well as base station antennas. "Although it is unknown whether children are more susceptible to radio-frequency exposure, they may be at increased risk because of their developing organ and tissue systems," the NRC stated in a press release. "Additionally, specific absorption rates for children are likely to be higher than for adults, because exposure wavelength is closer to the whole-body resonance frequency for shorter individuals. The current generation of children will also experience a longer period of RF field exposure from mobile-phone use than adults, because they will most likely start using them at an early age. The report notes that several surveys have shown a steep increase in mobile-phone ownership among children, but virtually no relevant studies of human populations at present examine health effects in this population."

Source: http://www.rcrnews.com/apps/pbcs.dll/article?AID=/20080118/FREE/192540885/1005

[Return to top]

Commercial Facilities Sector

29. *January 21, Daily News* – (New York) **Bomb-making factory found in Brooklyn apartment of Columbia professor.** Police stumbled upon a bomb-making factory Sunday in the home of a Columbia professor who specializes in the spread of infectious disease - and are investigating whether he and his roommate have terror ties. When investigators went to the 37-year-old's apartment, they found the bombs, already capped on both ends and filled with powder. One of the pipe bombs was inserted into a Nerf football, cops said. A 9-mm. handgun, two ammunition magazines, a 12-gauge shotgun, silencers, a bulletproof vest, a crossbow and bomb-making equipment, including a drill and threading machine that could be used to make pipe bombs, were also recovered, cops said.
Source: http://www.nydailynews.com/news/ny_crime/2008/01/21/2008-01-21_bombmaking_factory_found_in_brooklyn_apa-3.html

30. *January 18, Sheboygan Press* – (Wisconsin) **Explosion at Bemis injures worker.** A small explosion at a Bemis Manufacturing Co. plant in Sheboygan Falls, Wisconsin, Friday morning caused what appeared to be minor injuries to a 58-year-old male worker, according to authorities. The worker was performing routine maintenance on machinery in the regrind room at the wood flour mill when a small explosion of unknown origin caused damage to a door and injured the man, according to a Sheboygan Falls Police Department official. The incident was confined to the regrind room, he said, and a small fire that occurred after the incident was quickly extinguished by firefighters from Sheboygan Falls. Bemis is examining equipment to determine the cause of the explosion.
Source: http://www.sheboygan-press.com/apps/pbcs.dll/article?AID=/20080118/SHE0101/80118019

[Return to top]

National Monuments & Icons Sector

Nothing to report.

[Return to top]

Dams Sector

31. *January 18, Monterey County Herald* – (California) **Deadline set to pick plan to stabilize San Clemente Dam.** In California, completion of an environmental impact report on the San Clemente Dam has set the clock running for the state Department of Water Resources' Division of Safety of Dams to come up with a plan for how to

stabilize the dam. In 1992, the state Division of Dam Safety reported that the dam could give way in an earthquake of magnitude 5.5 on the Tularcitos Fault, which it straddles, or from a magnitude 7 quake on the San Andreas Fault. The chief of the Department of Water Resources' San Joaquin District certified the environmental report — prepared by Entrix Environmental Consultants for the state and the U.S. Army Corps of Engineers — effective December 31. Five alternatives to stabilizing the dam are up for consideration, said a senior engineer of the Dam Safety Division. One alternative that probably will not be considered, he said, is to do nothing. Other possibilities are shoring up the dam to strengthen it against a future earthquake; "notching," or cutting down the dam partway to relieve the pressure of accumulated water and silt behind it; tearing the dam down entirely and hauling off the sediment; and rerouting the Carmel River through San Clemente Creek by cutting away a spur of hillside that divides the two streams. A decision on which alternative will be selected must be made 180 days after the environmental report is certified, the engineer said, which is June 28. In fact, he said, the finding would have to be published 30 days before that date — May 29 — to allow time for public comment. San Clemente Dam was built in 1921 to hold back 2,000 acre-feet of water. Now its reservoir is filled with sediment and holds less than 100 acre-feet of water. The dam has been subject to overspilling during high flood seasons, according to state engineers, and water running over the top could erode rock on either side, causing the dam to break.
Source: http://origin1.montereyherald.com/ci_8006634?nclick_check=1

[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