Department of Homeland Security Daily Open Source Infrastructure Report for 25 January 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports a passenger bit a fellow traveler and then jumped out of a Continental Airlines jetliner as it was moving to take off from the Fort Lauderdale International Airport. (See item 8)
- The Columbus Dispatch reports the Ohio Department of Public Safety has unveiled a new center to identify possible terrorist activity by harnessing the power of state agencies that regulate agriculture, traffic, waterways, public health, and other areas. (See item 25)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

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 24, Associated Press* — **Fierce winds knock out power to 77,000 utility customers in California.** Fierce Santa Ana winds whipping through Southern California on Monday, January 23, fanned brush and house fires, knocked out power to 77,000 utility customers, and littered roads with palm fronds and trash cans. The dry wind, gusting near 70 mph in some places, roared out of the desert and down mountain passes and canyons to the coast, sending firefighters chasing outbreaks and toppling big rigs on highways. Most of the power outages were in San Gabriel Valley foothills and communities farther east. The La Canada Flintridge blaze was ignited by a fallen power line. Authorities were investigating whether the Tujunga

fire had the same cause. In Santa Ana, a freeway billboard blew over, broke a power pole in half and smashed a pair of RVs.
Source: http://www.latimes.com/news/nationworld/nation/wire/sns-ap-california-winds,1,1080160.story?coll=sns-ap-nation-headlines

2. *January 24, Associated Press* — **U.S. nuclear plant proposed, site identified.** Progress Energy Inc., has picked the site where it will seek to build the first nuclear reactor in the United States in more than 30 years. On Monday, January 23, the company chose an existing nuclear power site, its Shearon Harris plant near Raleigh, NC, for the possible construction. A final decision is years away on whether to actually build a new reactor there. An application to the Nuclear Regulatory Commission would arrive no sooner than late 2007, and if approved, construction could begin in 2010. The new reactor would not come on line until 2016. The utility, which operates five reactors at four locations and serves 1.4 million customers in the Carolinas, is among a handful of companies considering building a new reactor. Charlotte-based Duke Power, which serves 2.1 million customers in the Carolinas, is reviewing 14 potential sites. The last order for a new nuclear power plant came in 1973. Today, about 20 percent of the U.S. gets its electricity from nuclear reactors. Progress Energy said Monday there are plenty of factors that could stop the project — public and political support, growth and customer demand forecasts, and economic conditions.
Source: http://www.msnbc.msn.com/id/11005719/

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *January 24, Daytona Beach News-Journal Online (FL)* — **Tanker truck shuts down Florida interstate.** A tanker truck filled with 8,000 gallons of fuel burst into flames after it crashed in a southbound lane of Interstate 95 in Palm Coast, shutting down traffic in both directions for nearly an hour between U.S. 1 north of Flagler County and Palm Coast Parkway, FL. The single-vehicle accident occurred about 8 p.m. EST on I-95 a couple of miles north of the Palm Coast Parkway exit, said Debra Johnson, Flagler County Sheriff's Office spokesperson. The driver was airlifted to Halifax Medical Center. Nobody else was injured in the crash and fire. The fire was extinguished about 9:30 p.m. EST, and authorities opened one lane of traffic in the northbound direction. Johnson said all southbound lanes on I-95 were closed for hours. Southbound traffic north of the Flagler County line was diverted to U.S. 1 in St. Johns County and then back to I-95 just north of Ormond Beach.
Source: http://www.news-journalonline.com/NewsJournalOnline/News/Flagler/flaFLAG04012406.htm

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *January 24, Register (UK)* — **Yahoo! phishing warning.** Websense is warning of a new phishing scam targeting Yahoo! users. Users get a message via Yahoo!'s instant messenger asking them to "click on this website". Following the link takes you to what appears to be Yahoo!'s photo service. But the site is not associated with Yahoo!. Upon entering their user name and password users will receive an error message and their account details are forwarded to a third party.
   Screenshot of fake site: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =403
   Source: http://www.theregister.com/2006/01/24/yahoo_phishing_warning /

5. *January 24, Mercury News (Australia)* — **Scammers send fake Reserve Bank of Australia e−mails.** The Reserve Bank has been targeted by criminals trying to make cash from unsuspecting banking customers. A fake e−mail is being circulated purportedly on behalf of Australia's central bank urging people to reveal debit card details in a bid to counter money laundering and terrorism. Most Australian banks have been the target of similar scams, but this appears the first to bring in the Reserve Bank –− which does not deal with everyday banking customers. In the e−mail, which includes in its subject heading the term "verification required!", those behind the scam warn failure to reveal debit card details could result in the cessation of banking services for individuals. The fake e−mail reads, in part: "Criminal and terrorist elements have recently increased efforts to launder money through dormant debit−oriented accounts under the identities of deceased citizens and residents...In accordance with new anti−terrorism legislation aimed at preventing money laundering and financing of terrorist operations the Reserve Bank is working on behalf of Australia's financial institutions to verify customer debit cards." The e−mail comes under the name of a fraud squad commander. The bank said the e−mail was a fake and that it does not require verification such as debit card details.
   Source: http://www.themercury.news.com.au/printpage/0,5942,17921526, 00.html

6. *January 23, CNET News* — **Notre Dame probes hack of computer system.** Two computer−forensic companies are helping the University of Notre Dame investigate an electronic break−in that may have exposed the personal and financial information of school donors. The hackers may have made off with Social Security numbers, credit card information, and check images, Hilary Crnkovich, Notre Dame's vice president of public affairs, said. She declined to disclose how many donors may be at risk. Crnkovich said, "The (computer) server that was potentially affected was taken offline immediately...The university continues to explore safeguards and precautions to ensure something like this doesn't happen in the future." The student−operated newspaper at Notre Dame, The Observer, quoted donor and IT professional Mike Coffee wondering why a server storing sensitive information was connected to the Web. "It seems to be a very shoddy setup for protection of personal information." Crnkovich said that any donor whose checks were received by the school between Tuesday, November 22, 2005, and Thursday, January 12, 2006, may be at risk. The school said it has notified all the donors at risk.
   Source: http://news.com.com/Notre+Dame+probes+hack+of+computer+system/2100−1029_3−6030229.html?tag=cd.top

7.

January 23, TechWeb News — **Microsoft helps Bulgaria nab eight phishers.** Bulgarian authorities arrested eight people last week on charges that they were part of an international phishing ring that operated dozens of bogus Websites mimicking official Microsoft MSN pages. Dubbed the "MBAM Gang" by Microsoft −− for Microsoft Billing Account Management, the purported source of the phishing messages −− the group allegedly sent e−mails with spoofed MSN customer support addresses to dupe recipients into divulging credit card information. According to Bulgaria's National Services to Combat Organized Crime (NSCOC) agency, the stolen account data was used to purchase goods and make wire transfers of more than $50,000 from U.S., German, and British credit cards. Microsoft said that it provided information about the attacks to the NSCOC, as well as technical assistance during the investigation. Horacio Gutierrez, associate general counsel for Microsoft Europe, said, "Microsoft believes vigorous criminal enforcement against phishers is essential to show cybercriminals that there are consequences to their illegal actions."
Source: http://www.techweb.com/wire/security/177102753;jsessionid=15A1PFATTPMZMQSNDBCSKHSCJUMEKJVN

[Return to top]

Transportation and Border Security Sector

8. *January 24, Associated Press* — **Man jumps from moving jetliner onto tarmac.** An airline passenger bit a fellow traveler Monday, January 23, then jumped out of a jetliner as it was moving to take off, authorities said. The man was taken to a hospital from the Fort Lauderdale airport, the Broward County sheriff's office said. It was unclear whether he was injured. The other passenger suffered minor injuries from the bite. The Continental Airlines flight had been delayed for about 30 minutes, and as the Boeing 737 began to taxi, the man started yelling to get off, the sheriff's office said. He ran to the front of the plane and banged on windows and the cockpit door, authorities said. As passengers and crewmembers tried to restrain him, he bit a passenger. When the pilot depressurized the cabin, the man opened a door, jumped to the tarmac and ran toward the terminal. Deputies said they zapped him with a stun gun after he resisted arrest. Troy Rigby, 28, will be charged with criminal mischief, criminal trespass, battery, resisting arrest with violence and battery on a law enforcement officer, in addition to an outstanding warrant for marijuana possession, the sheriff's office said. The plane, set to fly from Fort Lauderdale−Hollywood International Airport to Newark, NJ, was carrying 116 passengers and five crewmembers.
Source: http://www.usatoday.com/travel/news/2006−01−24−passenger−jum ps_x.htm

9. *January 24, Department of Transportation* — **Gulf Coast states get $868 million to aid hurricane repair and reconstruction.** Gulf Coast states still rebuilding after last year's devastating hurricanes will share $868 million in federal funds aimed at aiding road and bridge projects, Department of Transportation Secretary Norman Y. Mineta announced Monday, January 23. Louisiana, Mississippi, Texas, and Florida will use the money to repair or rebuild federally supported highways and bridges damaged by Hurricanes Katrina and Rita, Mineta said. Mississippi will receive $740 million, Louisiana $75 million, Florida $42 million, and Texas $11 million for repairs based on formal requests already received from the states. Additional funds are likely to be received once the states issue final requests for aid, Mineta added. Eligibility for federal funds varies by project, but in most cases, the federal government

will pay for 100 percent of the work.
Source: http://www.dot.gov/affairs/dot0806.htm

10. *January 24, Associated Press* — **FBI: Border face−off involved men in Mexican military uniforms.** Men dressed as Mexican army soldiers, apparent drug suspects, and Texas law enforcement officers faced off on the U.S. side of the Rio Grande, an FBI spokesperson said Tuesday, January 24. Andrea Simmons, an agency spokesperson in El Paso, said that Texas Department of Public Safety troopers chased three SUVs, believing they were carrying drugs, to the banks of the Rio Grande during Monday's incident. Men dressed in Mexican military uniforms or camouflage were on the U.S. side of the border in Texas, she said. Simmons said the FBI was not involved and referred requests for further details to U.S. Immigration and Customs Enforcement.
Source: http://www.cnn.com/2006/US/01/24/mexico.border.ap/

[Return to top]

Postal and Shipping Sector

11. *January 24, Record – News (VT)* — **Mail delivery halted by BB−gun incident.** The U.S. Postal Service suspended delivery to a part of South Troy, VT, because a mail carrier was shot with a BB gun Friday afternoon, January 20. Some residents around the area then had to bring identification to pick up their mail at the post office. A 10−year−old was arrested Monday night, January 23. The child admitted to using his BB rifle to shoot street signs around 2 p.m. EST Friday when he accidentally struck mail carrier Tony Koumjian. A joint investigation between the Postal Service and the Troy Police Department, with the police doing most of the legwork and knocking on doors, led to the arrest around 6:30 p.m., said Troy Police spokesperson Det. Sgt. John Cooney. "It was a good cooperative effort between the agencies leading to some peace of mind for the neighborhood," said Cooney. More than 100 of the 27,000 Troy addresses that the Postal Service delivers to were affected by the suspension, said Postal Service spokesperson Maureen Marion. "From the Postal Service's perspective, whenever there's a safety issue we will suspend delivery in the area where that safety issue takes place until such time as we can come to a resolution."
Source: http://www.troyrecord.com/site/news.cfm?newsid=15987220&BRD=1170&PAG=461&dept_id=7021&rfi=6

[Return to top]

Agriculture Sector

12. *January 24, Stop Soybean Rust News* — **Soybean checkoff approves sentinel plots to fight soybean rust in 2006.** The more information on soybean rust, the easier it will be to control, which is why soybean checkoff farmer−leaders approved funds for additional sentinel plots to monitor the spread of soybean rust. Together the United Soybean Board (USB) and the North Central Soybean Research Program (NCSRP) will help establish sentinel plots from south to north in the Soybean Belt to monitor northward movement of soybean rust for early detection and early warning for soybean farmers. These plots will complement those established by the

U.S. Department of Agriculture (USDA). Timely detection of the disease can provide U.S. farmers with enough advanced warning to enable proper application of fungicides, the only effective management option for soybean rust at this time. Fungicides applied too late may be ineffective, and applications made too early could result in decreased efficacy and could result in the need for increased numbers of applications. Also, unnecessary treatments will result in higher input costs, hurting profitability. Between USDA, USB, and NCSRP, there will be a total of 20 sentinel plots established in most states. The checkoff will fund plots located in states where researchers believe USDA plot numbers may be insufficient.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=675

13. *January 24, Casper Star Tribune (WY)* — **Researchers look for missing link in elk die−off.** University of Wyoming researchers are looking for the “missing link” in the deaths of about 350 elk in early 2004 in south−central Wyoming. This month they launched a second major study to determine what caused some of the elk using the Red Rim/Daley Wildlife Habitat Management Area to lose their leg strength and coordination. They died of starvation or predation. College of Agriculture scientists, in collaboration with the Wyoming Game and Fish Department, previously determined the elk consumed Xanthoparmelia chlorochroa, a free−living lichen common in many parts of the state. They identified usnic acid, which is linked to liver damage in humans, in samples of the lichen collected from the Red Rim. Merl Raisbeck, a faculty member in the College of Agriculture’s Department of Veterinary Sciences, said his team believes usnic acid is only partly responsible for the elk deaths. According to laboratory experiments, the amount of acid in lichen collected from the area could not have been solely responsible for the poisonings, Raisbeck said. "It is probable that usnic acid acted in synergy with some other, as yet unidentified, toxin to cause the syndrome seen in the field,” Raisbeck said.
Source: http://www.casperstartribune.net/articles/2006/01/24/news/wyoming/fec7e866e17356b28725710000028b49.txt

14. *January 24, Agricultural Research Service* — **New technology improves ranch management.** New technology developed by the Agricultural Research Service (ARS) predicts forage growth, allowing ranchers to make more−informed management decisions. At the ARS Great Plains Systems Research Unit (GPSR) in Fort Collins, CO, soil scientist Gale Dunn and range systems modeler Allan Andales are developing a database that will analyze historical and simulated data. The database will predict future forage growth and help ranchers decide how many animals to graze on native range. The new database is based on GPFARM, a computer simulation model developed at GPSR to help central Plains farmers and ranchers make management decisions. GPFARM interprets data and predicts the outcomes of various management strategies. But its complexity intimidates many farmers and ranchers, decreasing its efficacy. According to Dunn, ranchers, in particular, were missing the program’s benefits. So he submitted a proposal to the U.S. Department of Agriculture’s Risk Management Agency and received $570,000 to develop and deliver a database to help ranchers manage range and livestock production systems. The program will predict the effects of drought on range, forage, and livestock production. This new system will be simpler than GPFARM. Instead of running a simulation model, the rancher will only need to submit questions to the database.
Source: http://www.ars.usda.gov/is/pr/2006/060124.htm

15.

January 23, Associated Press — **Research facility fills up with Yellowstone bison.** A research site north of Yellowstone National Park has filled to capacity with young bison that will be used in studying whether brucellosis−free herds can be produced from quarantine. The 48 bison calves shipped to the site at Corwin Springs, MT, over the weekend brings to 100 the total number of young bison being held at the site, said Mel Frost, a spokesperson for the state Department of Fish, Wildlife and Parks. Thirty−eight bison, also captured this winter near the park's northern border after venturing too far, were sent over earlier. The bison join 14 others that were captured last year, she said. The state−federal project is looking at whether a so−called quarantine facility could be useful both in finding bison free of the disease brucellosis and in helping set up brucellosis−free herds in Montana and other states. Researchers began accepting bison calves captured near the park's borders last year. Bison can be captured under a joint state−federal management plan aimed at reducing the potential spread of brucellosis from wandering bison to cattle in Montana. Brucellosis is found in the park's bison herd and in elk in the region. To qualify for quarantine, bison calves must test negative for brucellosis.
Brucellosis information: http://www.aphis.usda.gov/vs/nahps/brucellosis/
Source: http://www.billingsgazette.com/index.php?tl=1&display=rednews/2006/01/23/build/state/21−bison.inc

[Return to top]

Food Sector

16. *January 24, Agence France−Presse* — **South Korea calls off beef talks with Canada.** South Korea has decided to call off talks with Canada on the resumption of beef imports after a fresh case there of mad−cow disease. The Agriculture Ministry said it would put off planned beef talks with Canada, originally scheduled for February. Canada confirmed Monday, January 23, that a six−year−old cow became its fourth recorded mad−cow case after it showed symptoms of bovine spongiform encephalopathy. South Korea suspended U.S. and Canadian beef imports in 2003 after mad−cow cases were discovered in animals in the two countries. At talks with the U.S. two weeks ago, South Korea agreed to lift the ban on some U.S. beef products starting in March.
Source: http://www.todayonline.com/articles/97090.asp

17. *January 23, Food Safety and Inspection Service* — **Pot stickers recalled.** Nestle Prepared Foods company, a Gaffney, SC, firm, is voluntarily recalling approximately 54,690 pounds of frozen LEAN CUISINE® Asian−Style pot stickers due to the possible presence of pieces of plastic, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Monday, January 23. The recall was prompted by consumers reporting small pieces of plastic in the meals. FSIS has received no reports of injury from consumption of this product. The pot stickers were produced on September 19, 2005, and were distributed to retail stores nationwide.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_002_2006_relea se/index.asp

18. *January 20, U.S. Food and drug Administration* — **California Health Department issues warning on juice.** Consumers should not drink Evolution, Harvest or Trader Joe's brand assorted juices manufactured by Juice Harvest Corp. of San Bernardino, CA, because the products were not fully pasteurized and may contain harmful bacteria that pose a health risk,

California Public Health Officer Mark Horton announced Friday, January 20. No illnesses associated with these products have been reported. Approximately 8,000 units of the assorted juices distributed in Southern California are being voluntarily recalled. The California Department of Health Services is investigating to determine which distributors and retail establishments received these products.
Source: http://www.fda.gov/oc/po/firmrecalls/juiceharvest01_06.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

19. *January 24, Reuters* — **Asian states slow to report bird flu.** Asian countries have taken too long to report some human cases of bird flu and this could harm efforts to contain any future pandemic, a top World Health Organization (WHO) official said on Tuesday, January 24. Shigeru Omi, the WHO's Western Pacific regional director, said the failing showed the need for countries to improve their ability to detect and report cases of the H5N1 virus rapidly. "The window of opportunity for containment is very narrow, meaning rapid containment measures must be carried out at least two to three weeks after detection of a potential pandemic event," Omi said in a speech to the WHO's Executive Board. "However up to now, only half of the reports for human H5N1 cases meet this target. Some reports have been received as late as one or two months after disease onset," he added. The bird flu virus has killed at least 82 people in six countries since late 2003.
Source: http://today.reuters.com/news/newsArticle.aspx?type=worldNews&storyID=2006-01-24T171537Z_01_L24327168_RTRUKOC_0_US-BIRDFLU-WHO.xml&archived=False

20. *January 24, Reuters* — **Anti-viral drug now being shipped to all markets.** Swiss pharmaceutical company Roche Holding AG on Tuesday, January 24, said it has lifted restrictions on the distribution of influenza treatment Tamiflu and is now shipping orders to all markets. The company said it previously was distributing Tamiflu only to U.S. cities where a high incidence of influenza was being reported. The drug has been in high demand amid concerns about a possible bird flu pandemic in people. Roche said it made the decision after seeing an increase in flu reports in the U.S. and a Centers for Disease Control and Prevention advisory to doctors to avoid using two older flu drugs this season.
Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006-01-24T164405Z_01_WEN8449_RTRUKOC_0_US-ROCHE.xml&archived=False

21. *January 23, Times-Picayune (LA)* — **Storms put dent in West Nile virus.** Hurricanes Katrina and Rita pounded southern Louisiana last year, but the water they dumped on the state did not lead to a surge in West Nile virus infections, according to the state health department's

year−end report on the mosquito−borne disease. Even though the insects breed in water, the storms flushed out the stagnant areas they like for breeding, killed adult mosquitoes, washed away larvae, and killed or dispersed the birds that carry West Nile after mosquitoes bite them, state epidemiologist Raoult Ratard said. According to the summary, 177 Louisianans were infected with West Nile last year and 10 people died from its complications. The last case count represented an increase of 22 infections since the previous report in mid−November. There were only scattered reports of infections last year in the New Orleans area, where Katrina struck, and southwest Louisiana, where Rita roared ashore, Ratard said. In the seven−parish New Orleans area, there were 26 infections and one death, which occurred in Orleans Parish in July. The statewide case total was the highest since 2002, when West Nile infections were first reported in Louisiana. In that year, there were 329 cases and 25 deaths.
Source: http://www.nola.com/news/t−p/metro/index.ssf?/base/news−12/1137999376140350.xml

22. *January 23, National Institute of Allergy and Infectious Diseases* — **Studies illustrate potential of chimp/human antibodies to protect against smallpox.** Results from a new study performed in mice indicate that hybrid laboratory antibodies derived from chimpanzees and humans may provide a safe and effective way to treat the serious complications that can occur following smallpox vaccination −− and possibly may even protect against the disease itself. The current smallpox vaccine consists of a live but weakened strain of vaccinia virus, a relative of the variola virus that causes smallpox. Vaccinia immunization has been proven effective in generating immunity against smallpox virus. Although most reactions to the vaccinia virus are mild, the vaccine can cause serious and even life−threatening complications in individuals with weakened immune systems or skin conditions, in infants younger than 12 months, and in pregnant women. Smallpox vaccine complications are currently treated with anti−vaccinia immune globulin (VIG) −− pooled antibodies taken from the blood of individuals immunized with the smallpox vaccine. However, VIG is in short supply since the U.S. discontinued public smallpox vaccinations in 1972. Researchers developed hybrid antibodies from chimpanzees and humans that effectively inhibited the spread of both vaccinia and variola viruses in test tube experiments. Moreover, the hybrid antibodies proved more effective than VIG when tested in mice infected with vaccinia virus, even when given two days after virus exposure.
Source: http://www.nih.gov/news/pr/jan2006/niaid−23.htm

[Return to top]

Government Sector

23. *January 24, Statesman Journal (OR)* — **Oregon courthouse upgrade estimates reviewed.** Marion County commissioners got a glimpse Monday, January 23, at the cost of buying new security barriers, repairing leaky windows, and expanding the entrance at the courthouse. Courthouse upgrades could end up costing about $2.5 million to $2.7 million. Some of the projects are a response to events in which a man smashed through the courthouse with a pickup and set fire to the building, according to police. The rough estimate doesn't include multimillion−dollar courthouse repairs needed because of the alleged rampage. Insurance will cover most of those. Upgrades discussed Monday include a marble planter and other barriers to stop anyone from ramming the entrance with a vehicle again. The barriers should cost less than $10,000, said Gayle Horton, the county business−services director. Also, expanding the

courthouse entrance will cost of $350,000 to $450,000. Officials want a larger entrance that can hold more people and allow them to be screened more quickly.
Source: http://159.54.226.83/apps/pbcs.dll/article?AID=/20060124/NEW S/601240317/1001

[Return to top]

Emergency Services Sector

24. *January 24, Providence Journal (RI)* — **Rhode Island officials practice response to dam failure.** If the Upper Pascoag Reservoir Dam in Providence, RI, failed and flooded Pascoag Village, there could be up to 600 casualties and about 1,000 evacuees, according to the town's Emergency Management Director Richard J. Lapierre. Last Thursday, January 19, the town's Emergency Management Agency conducted its first disaster exercise, testing how well department officials work with one another and how effective the disaster response is. The dam is one of 17 high−hazard dams, defined as structures that, if breached, could cause significant loss of life or economic damage. The exercise was moderated by James Miskel, a former instructor at the Navy War College in Newport who works as a consultant for the Rhode Island Department of Emergency Management. According to the scenario, the dam was destroyed by a terrorist attack. Miskel posed different challenges to the heads of the town's fire, police, rescue, public works, and administrative departments. Among the challenges thrown at them were loss of electricity, telephone service, or specific roads in town that lie in the flood plain. Lapierre said the town needs to work on its communication between departments and its ability to work with other towns and local volunteers who might help during a disaster.
Source: http://www.projo.com/northwest/content/projo_20060124_bdam.d abdff4.html

25. *January 24, Columbus Dispatch (OH)* — **Ohio launches anti−terror nerve center.** Tuesday, January 24, the Ohio Department of Public Safety unveiled a new center to identify possible terrorist activity by harnessing the brainpower of state agencies that regulate agriculture, traffic, waterways, public health and other areas. The Ohio Strategic Analysis and Information Center is being launched with $290,000 in federal funding for equipment and $300,000 for personnel, although most of its 10 to 12 regular employees will continue to draw their paychecks from participating state agencies. "A traditional information center [only] has law enforcement in it," said Richard Rawlins, the Ohio Homeland Security deputy director who will run the center. "We found after 9/11 that we need to do a lot better." Rather than creating a large bureaucracy, the center will function as a terrorism nerve center for state government, allowing agencies that rarely interact to swap intelligence that might stop terrorists.
Source: http://www.columbusdispatch.com/news−story.php?story=dispatch/2006/01/24/20060124−A1−02.html

[Return to top]

Information Technology and Telecommunications Sector

26. *January 24, PC World* — **Spammers will innovate, morph, and adapt in 2006.** Representatives at several ISPs say they are gearing up for new challenges in 2006, when they expect spammers to grow more sinister. AOL spam fighters say that 2006 will be the year of

the zombie networks. Zombie PCs are computers that have been infected by malicious code that allows spammers to use them to send e−mail. AOL also says that in 2006 there will be more "special−order" spam, in which phishers play off of your security concerns, especially the fear that your identity has already been stolen. Viruses and worms that take advantage of security holes in Microsoft's Outlook and Internet Explorer are a given for 2006, say experts. Richi Jennings, analyst at Ferris Research, says the recent Windows Metafile Format flaw is a perfect example. Also experts predict a new spam theme this year. In 2005 spam pitches ranged from cable descramblers to "free" iPods. But in 2006 spammers will be promoting things like investment opportunities and pumping penny stocks instead of pushing products. This is likely because it's extremely hard to differentiate a real stock tip from your broker as opposed to a fake one from a spammer, AOL says.
Source: http://www.pcworld.com/news/article/0,aid,124408,00.asp

27. *January 23, Associated Press* — **Botnet hacker pleads guilty.** A 20−year−old hacker admitted Monday, January 23, to surreptitiously seizing control of thousands of Internet−connected computers, using the zombie network to serve pop−up ads and renting it to people who mounted attacks on Websites and sent out spam. Jeanson James Ancheta, of Downey, CA, pleaded guilty in Los Angeles federal court to four felony charges for crimes, including infecting machines at two U.S. military sites, that earned him more than $61,000, said federal prosecutor James Aquilina. Prosecutors called the case the first to target profits derived from use of "botnets," large numbers of computers that hackers commandeer and marshal for various nefarious deeds. The "zombie" machines' owners are unaware that parasitic programs have been installed on them and are being controlled remotely. Ancheta one−upped his hacking peers by advertising his network of "bots," short for robots, on Internet chat channels. A Website Ancheta maintained included a schedule of prices he charged people who wanted to rent the machines, along with guidelines on how many bots were required to bring down a particular type of Website. Acheta's sentencing is scheduled for May 1.
Source: http://www.cnn.com/2006/TECH/internet/01/23/hacker.ap/index. html

28. *January 23, IDG News Service* — **Four new Trojans on the loose.** Four new Trojans are on the loose, three aimed at mobile phones and a fourth at PCs, anti−virus companies have warned. The mobile phone worms are disguised as legitimate applications and spread via Bluetooth or multimedia messages and affect phones running Symbian. The computer worm spreads via e−mail and purports to offer pornography. The phone worms −− Bootton.E, Pbstealer.D and Sendtool.A −− have a low infection rate at the moment. The first was spotted last week by F−Secure and Symantec and is perhaps the most potentially crippling of the three to those infected. It restarts the mobile but also releases corrupted components that cause a reboot to fail, leaving the device unusable. Fortunately, the phone worms are unlikely to spread very far. Unlike worms on computers, the Trojan horses hitting cell phones spread as attachments that require users to download them. The PC worm, Nyxem, however, is spreading rapidly and carries a potentially destructive set of instructions. Also nicknamed the Kama Sutra worm, it is programmed to overwrite all of the files on computers it infects on Friday, February 3, said Mikko Hypponen, chief research officer at F−Secure Corp. So far, there's no indication where Nyxem originated.
Source: http://www.techworld.com/security/news/index.cfm?NewsID=5219

29.

January 23, Associated Press — **Supreme Court won't hear BlackBerry appeal.** Millions of BlackBerry users can now turn their attention back to a Richmond, VA, federal court where the fate of the popular wireless e−mail device may be decided after the Supreme Court chose on Monday, January 23, to not intervene in the case. Many analysts expect Research In Motion Ltd. (RIM), the device's maker, to strike a deal with the patent−holder or introduce changes to work around the patents. Lawyers for NTP Inc., a small northern Virginia firm that says it owns the patent on the technology that makes the BlackBerry work, have said government and emergency workers would be exempt from any BlackBerry blackout. At issue was how U.S. law applies to technology that is used in a foreign country and allegedly infringes on the intellectual property rights of a patent−holder in the U.S. RIM, a Canadian company, had contended it cannot be held liable for patent infringement because its main relay station for e−mail and data transmission is located in Waterloo, Ontario, outside U.S. borders. But a federal appeals court had found that the Canadian company had infringed on the patents held by NTP because customers use the BlackBerry inside U.S. borders.
Source: http://www.nytimes.com/aponline/technology/AP−Scotus−BlackBerry−Battle.html?_r=1

30. *January 23, Reuters* — **T−Mobile seeks to halt cell phone record sales.** T−Mobile, the No. 4 U.S. wireless carrier, said on Monday, January 23, it asked a Washington state court to prevent companies from allegedly using fraudulent means to obtain and sell T−Mobile customer call records. German−owned T−Mobile said it asked the court for an injunction against Data Find Solutions, 1st Source Information Specialists and related firms and individuals. T−Mobile said the companies ran or owned Websites such as www.locatecell.com and www.celltolls.com that offered such services. The lawsuit was filed in King County, Washington Superior Court, under the state's criminal profiteering laws, said T−Mobile, which is owned by Deutsche Telekom. "To further safeguard the privacy of our customers, T−Mobile is taking action to prosecute these online data brokers to the fullest extent permitted by the law," Dave Miller, T−Mobile's senior vice president and general counsel, said in a statement. U.S. lawmakers, state attorneys general, and the Federal Communications Commission are looking into what laws, if any, were broken by companies that have obtained cell phone records and sold them. Officials are concerned companies are posing as customers or phone company employees to gain access to call records and then selling them online.
Source: http://today.reuters.com/investing/financeArticle.aspx?type=bondsNews&storyID=2006−01−24T002714Z_01_N23191368_RTRIDST_0_TELECOMS−TMOBILE−RECORDS.XML

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a public exploit for a vulnerability in VERITAS NetBackup Volume Manager Daemon (vmd). The VERITAS NetBackup vmd listens on network port 13701/tcp. An attacker could

send a specially crafted packet to the Volume Manager on a vulnerable system to cause a buffer overflow or a denial of service condition. Successful exploitation may allow may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system with root or SYSTEM privileges. More information about this vulnerability can be found in the following URL:

VU#574662 VERITAS NetBackup library buffer overflow vulnerability:
http://www.kb.cert.org/vuls/id/574662

US−CERT strongly encourages users and administrators to review the following mitigation to address this vulnerability as soon as possible:

Review the Symantec Advisory SYM05−024 and apply the recommended updates to address this vulnerability:

http://seer.support.veritas.com/docs/279553.htm

http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNL OAD.htm

Restrict access to the ports used by the NetBackup services.

Current Port Attacks

Top 10 Target Ports	6881 (bittorrent), 1026 (win−rpc), 53 (domain), 445 (microsoft−ds), 139 (netbios−ssn), 4672 (eMule), 1434 (ms−sql−m), 161 (snmp), 1027 (icq), 6346 (gnutella−svc) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[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 dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 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