Department of Homeland Security Daily Open Source Infrastructure Report for 18 January 2006

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Daily Highlights

- Department of Homeland Security Secretary Michael Chertoff and Secretary of State Condoleeza Rice announced a joint agenda for securing borders and opening doors to those who lawfully cross the borders of the United States. (See item 17)
- Agence France−Presse reports officials from 90 countries and 25 organizations gathered on Tuesday, January 17, in Beijing for two−day international meeting that planned to raise 1.5 billion dollars to help fight bird flu. (See item 29)

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 17, Associated Press* — **Transmission network held up during ice storm.** Public Service Commissioners (PUC) gave utility companies high marks after watching a show−and−tell on the late November ice storm that knocked out power to thousands for more than a week in North Dakota, South Dakota, and Minnesota. The storm but could have been worse, Commissioner Kevin Cramer said. "The fact that they were able to avoid rolling blackouts, the fact that the system has the capacity as well as the management to be able to shift and adjust, is very reassuring," he said. Several large energy users cut back on electricity, especially when a major transmission line went down for about 36 hours. Area linemen assisted

in restoring power. The storm showed a need to upgrade some major transmission lines, especially in the region's eastern area, said Tony Clark, PUC president. Said Clark, "You can see pretty graphically the need for updating lines in Minnesota...It's a regional issue, so to the extent any of our companies are investing, we're going to be asked to chip in for it." Commissioners said expanding transmission routes would help guard against one major event taking out a large area. Clark said it was most important that utilities have a plan to deal with outages.
Source: http://www.wctrib.com/ap/index.cfm?page=view&id=D8F68A6O0

2. *January 17, Times Online (UK)* — **Shell pulls out staff after attacks leave Nigerian oilfields facing paralysis.** Separatist rebels in Nigeria were close to achieving their aim of paralyzing oil production in the Niger delta after Shell made a partial evacuation of 326 oil workers on Monday, January 16, following attacks on its facilities by heavily armed militants. Shell acted after a speedboat attack on Sunday, January 15, on one of its pumping stations off the port of Warri left an unknown number of people dead. Its response to the fourth attack in five days alarmed international oil markets, already jittery over the West's nuclear standoff with Iran. Nigeria, the world's eighth−largest oil exporter, produces 2.4 million barrels of oil a day. Most of its crude goes to the United States. Shell, the largest oil producer in Nigeria, said it had no plans to quit the delta but refused to rule out further evacuations. According to a company press release, all four flow stations had already been closed because of the attack on the Trans Ramos pipeline, and withdrawing staff would have no new impact on production. The militant group said in an e−mail statement, "Our aim is to totally destroy the capacity of the Nigerian Government to export oil."
Source: http://www.timesonline.co.uk/article/0%2C%2C3−1988746%2C00.h tml

3. *January 17, Rutland Herald (VT)* — **Police arrest 11 during nuke protest.** Eleven people were arrested for trespassing Monday morning, January 16, at the front door of Entergy Nuclear. Over 100 people were also part of a larger protest. Monday's demonstration at the offices of the owner of the Vermont Yankee nuclear power plant was the third and largest of the most recent string of protests organized by the anti−nuclear group Citizens Awareness Network (CAN) and the Traprock Peace Center, both Massachusetts−based organizations. Deb Katz, executive director of CAN, said that protests are already planned for February and March. Entergy spokesperson Robert Williams declined to comment about the protest. "Our focus is on safely operating the plant," he said. Entergy security personnel kept a much lower profile than in the previous protests. Brattleboro police chief John Martin, contacted after the protest, said that the protests were beginning to be a burden on the small−town police department. During the morning protest, the department had three accidents, one 911 emergency call, and an ambulance call −− with only one officer to cover those emergencies while three officers were at Entergy.
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/2006 0117/NEWS/601170365/1003

4. *January 15, Financial Times (UK)* — **Power companies predict return to coal.** The world is on the brink of a big switch from gas to coal as the preferred fuel for power stations, according to projections from Alstom, Siemens, and General Electric, the world's three biggest power equipment makers. Independent forecasts from France's Alstom and Germany's Siemens show that about 40 percent of the orders for electricity turbines in the next decade will be for

coal−powered units, with the share of gas−fired plants falling to between 25 and 30 percent. Philippe Joubert, president of Alstom's power division, said, "The structure of the power market is seeing a radical shift away from gas and towards coal." Siemens' figures point to a similar conclusion, while GE said it expected to see a "more balanced picture" in terms of equipment orders, with gas being far less dominant than recently. The shift is being triggered by technological changes and by rising disenchantment with gas as a fuel. Concerns exist over rising natural gas prices and worries about security of supply. Many countries in Asia, which is expected to provide half of all new power station orders in the next 10 years, lack ready access to gas reserves.
Source: http://news.ft.com/cms/s/69c23e40−8602−11da−bee0−0000779e234 0.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *January 17, WPXI (PA)* — **Acid leaks from derailed train in Pennsylvania.** Emergency crews were called to the scene of a train accident in Lawrence County, PA. Officials said that a few cars derailed at about 10:30 a.m. EST Tuesday, January 17, in West Pittsburgh, just outside of New Castle. One of those cars contained sulfuric acid and was leaking. So far, no injuries have been reported. Sulfuric acid is not combustible, but the material is corrosive and very toxic.
Source: http://www.wpxi.com/news/6180693/detail.html

6. *January 16, Associated Press* — **Gasoline tanker truck overturns in New York, catches fire.** A tanker truck carrying thousands of gallons of gasoline overturned on a major Queens, NY, highway on Monday, January 16, and caught fire, burning down an overpass and spewing thick black smoke that could be seen for miles. The driver, who suffered minor injuries, was able to walk away from the crash, said Jim Tuller, chief of the police department's Queens North Bureau Command. No one else was injured. The Mobil truck was carrying 8,000 gallons of gasoline when it overturned just before noon EST near the Roosevelt Avenue exit of the six−lane Brooklyn−Queens Expressway in Queens, said Michael Lee, a director at the city's Office of Emergency Management. No other vehicles were involved. The fire was extinguished by Monday evening but started again around 9 p.m. EST, when sparks from a cleanup worker's torch ignited a pool of water and gasoline. The No. 7 subway line, which runs on elevated tracks just beyond the overpass, was shut down in both directions between Queensboro Plaza and Willets Point, first for several hours because of concern that sparks from subway tracks could land on the spill and then briefly because of the reignited fire.
Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−tankerfire0116jan16,0,5691541.story?coll=ny−region−apnewyork

7. *January 16, Associated Press* — **Gas leak shuts down Massachusetts subway station, diverts passengers.** A gas leak at the Shawmut subway station in Boston, MA, closed the station and diverted passengers. According to a Massachusetts Bay Transportation Authority spokesperson, a contractor working on renovations at the station Monday morning, January 16, struck a gas line causing the leak. There were no injuries. The station was closed and passengers are being bussed between Ashmont and JFK/UMass on the red line.
Source: http://www.boston.com/news/local/massachusetts/articles/2006

/01/16/gas_leak_shuts_subway_station_diverts_passengers/

8. *January 12, Dispatch (NC)* — **North Carolina businesses evacuated because of propane leak.** A hosiery building on Salisbury Street in Denton, NC, and a nearby BB&T branch bank office were evacuated Wednesday afternoon, January 11, after a propane tank outside of Century Hosiery sprung a leak and caught fire. The call about the fire came into the Emergency Communications Center at 1:05 p.m. EST and the fire was under control by 1:18 p.m., according to emergency services. The leak was capped by fire officials. No one was injured and there was no property damage reported.
Source: http://www.the−dispatch.com/apps/pbcs.dll/article?AID=/20060112/NEWS/601120340/1006/NEWS02

[Return to top]

Defense Industrial Base Sector

9. *January 13, Journal of Net−Centric Warfare* — **Vision statement for U.S. Geospatial Intelligence released.** The National Geospatial−Intelligence Agency (NGA) in Bethesda, MD, recently released its November 2005 “Statement of Strategic Intent,” which it calls a vision for the future of geospatial intelligence (GEOINT). The latter refers to the combination of imagery, imagery intelligence and geospatial data. NGA said the document “reflects changes in the Intelligence Community and responds to challenges from oversight commissions to embrace innovative analytic approaches and improved information sharing and collaboration.” NGA’s director, retired Air Force Lt. Gen. James R. Clapper Jr., identified the following goals in the 2005 Statement of Strategic Intent: 1) Establish an integrated, collaborative analysis and production environment that is responsive to and predictive of continuing and emerging global threats; 2) Institute and expand an interoperable, strategically aligned [cross−governmental] National System for Geospatial Intelligence (NSG); 3) Attract, develop, sustain and engage a workforce with the skills and competencies required to meet current and future threats and challenges; 4) Identify, develop, acquire and deploy capabilities and technologies to anticipate and meet the ever−increasing demand for timely, relevant and accurate GEOINT.
NSG Statement of Strategic Intent:
http://www.nga.mil/NGASiteContent/StaticFiles/OCR/nsg_strate gic_intent.pdf
Source: http://www.isrjournal.com/story.php?F=1466244

[Return to top]

Banking and Finance Sector

10. *January 17, Government Technology* — **California's new anti−phishing law takes effect this month.** California legislation that took effect this month includes a new law against "phishing" intended to protect consumers. Senate Bill 355 makes Internet phishing a crime in California. Phishing is the practice of using e−mail to entice recipients to divulge personal information, such as Social Security numbers or credit card numbers, in order to commit fraud.
Senate Bill: http://www.leginfo.ca.gov/pub/bill/sen/sb_0351−0400/sb_355_bill_20050930_chaptered.pdf

Source: http://www.govtech.net/news/news.php?id=97895

11. *January 16, Silicon.com* — **Criminals make 20,000 false tax credit claims in UK.** More than half of 40,000 suspicious tax credit applications detected by the United Kingdom's HM Revenue and Customs (HMRC) during a six−month period last year are believed to have been made by organized criminal gangs, new government figures have revealed. The huge rise in fraud attempts forced HMRC to close the online tax credits portal at the beginning of December last year after it discovered personal details of 13,000 civil servants had been stolen and used by criminals to make false claims. HMRC admits it still does not know the full extent of the fraud. The department has now revealed it intervened in 38,924 suspicious claims between April and November last year before they got to payment stage. Dawn Primarolo, paymaster−general, said more than half of these claims were the result of organized attacks, and HMRC intervened in another 22,380 cases where tax credit was already in payment and fraud was suspected during the same period. The tax credit Website handles around half a million transactions per year and the scammers were able to change claim details and redirect the money into their own bank accounts acquiring a genuine claimant's name, birth date, and national insurance number.
Source: http://www.silicon.com/publicsector/0,3800010403,39155645,00 .htm

12. *January 16, Internetnews* — **Online shopping boosted by security confidence.** A new Business Software Alliance (BSA) study conducted by Harris Interactive reports that 70 percent of respondents felt little security concern in making online purchases in 2005. Thirty−eight percent reported that they spent more online in 2005 than they did in 2004. Concerns about Internet security for online holiday shopping ran highest with older Americans (55 and older). Part of the reason why security concerns were not an obstacle is due to a high degree of confidence in computer security mechanisms. Fifty−six percent they were either very or extremely confident that they were protected from computer viruses. Respondents were similarly confident in their protection from credit card fraud (50 percent), identity theft (46 percent), and spyware (41 percent). Most (88 percent) have anti−virus protection, 78 percent have anti−spyware software, and 77 percent reported having a firewall. The same percentage indicated they use spam−filtering software. "We don't doubt that the wide availability of effective security software products that detect and fight cyber security threats is helping to restore consumer confidence in the security of online transactions," said Diane Smiroldo, BSA's vice president of public affairs. The survey solicited the opinions of 2,152 U.S online adults from December 27−29.
Study: http://www.bsacybersafety.com/news/2005−Online−Shopping−Conf idence.pdf
Source: http://www.internetnews.com/security/article.php/3577631

13. *January 15, Associated Press* — **Wave of scam e−mails popping up in inboxes from Russia to Kentucky.** Following up on the politically charged jailing of oil tycoon Mikhail Khodorkovsky, a wave of scam e−mails in the style of Nigeria's notorious spammers have been popping up in inboxes from Moscow to Kentucky. One letter from "Leila Khodorkovsky," claiming to be the billionaire's wife requests assistance investing $45 million of the tycoon's money and promises compensation. Another is signed by "Larissa Sosnitskaya," who describes herself as a personal treasurer to Khodorkovsky, seeking a beneficiary for a similar sum. Worth $15 billion before his arrest, Khodorkovsky was an obvious choice for the authors of the Nigerian−style spam, experts say. "This is a well−developed business they choose what is up−to−date," said Yevgeny Altovsky, who coordinates a UNESCO−backed anti−spamming

program in Moscow. He said, "The main thing is it has to involve some kind of rich person...If a major court case against Bill Gates were to start tomorrow I'm sure he would appear in these messages."
Source: http://abcnews.go.com/Technology/wireStory?id=1509294

14. *January 15, Alaska Journal of Commerce* — **Banks stress vigilance as online fraud scams increase.** Four times in five weeks, someone went phishing for information from Credit Union 1 (CU1) members. It's likely that thousands of Alaskans received e−mail messages last month that aimed to bait them into giving up their log−in passwords, personal identification numbers, and credit card information. When a member clicked on the link, he was taken to a Website that closely resembled that of Credit Union 1, and was asked to supply names, phone numbers, and e−mail addresses. Another field asked for credit card information, including expiration dates, ATM PINs, and online passwords. Pat Berry, CU1's internal auditor and security officer, said a couple members had money stolen from their accounts. Credit Union 1 isn't the only financial institution in Alaska targeted for phishing scams. Alaska USA Federal Credit Union and First National Bank were also targeted in 2005. "People will use any underhanded method −− fear, intimidation, build trust −− to get people to divulge information," said Erik Bjella, spokesperson for First Bank. Cherri Gillian of First National Bank of Alaska, said "[Online fraud] exposes us and we're responsible for our shareholders' investments and our customers."
Source: http://www.alaskajournal.com/stories/011506/hom_20060115010. shtml

[Return to top]

Transportation and Border Security Sector

15. *January 17, Associated Press* — **In bankruptcy, radical changes brew for Northwest, unions.** Northwest Airlines wants to shift midsize jet flying and some baggage handling work to subsidiaries, angering pilots and ground workers. And it wants to shift thousands of U.S.−based, union−covered flight attendant jobs to foreign hires. The centerpiece is the idea for a new regional carrier, dubbed NewCo for now. "NewCo represents the cornerstone of our domestic renewal," said Tim Griffin, executive vice president for marketing and distribution. Northwest is trying to negotiate those changes into new contracts along with steep pay cuts and other givebacks by workers. A trial on the issue began Tuesday, January 17, in New York. NewCo with a fleet of new 70− to 100−seat jets could have as many as 105 aircraft by 2010, and would fly under its own Federal Aviation Administration operating certificate. Northwest President and Chief Executive Doug Steenland said the jets are the perfect size for 20 percent of Northwest markets, which include more small cities than any other carrier. Northwest has promised to staff NewCo with pilots it furloughed in the industry downturn that began in 2001. Northwest said most other airlines use outside carriers for flying those midsize jets, but its current pilot contract makes that too expensive.
Source: http://www.usatoday.com/travel/news/2006−01−16−nwa−changes_x .htm

16. *January 17, NorthJersey.com* — **Faulty landing shuts Teterboro.** A twin−engine plane's nose gear collapsed as it landed at Teterboro Airport on Monday evening, January 16, forcing officials to close the airport for an hour. There were no injuries or fire in the incident, said Pasquale DiFulco, a spokesperson for the Port Authority, which operates the airport. There were no passengers aboard the plane. The airport was closed for an hour, but officials did

"reopen one runway" while the plane was moved, DiFulco said. This latest incident raised a red flag with out−going New Jersey Governor Richard Codey, who said he would call Port Authority Chairman Anthony Coscia to discuss proposed safety upgrades at the airport. "The situation is out of control," Codey said, referring to several accidents in 2005, including one February 2 when a chartered corporate jet sped off the runway and barreled across six lanes of Route 46 before crashing into the Strawberry clothing warehouse after an aborted takeoff. Codey, noting that the airport is located in a densely populated region of Bergen County −− its 827 acres occupy parts of Teterboro, Moonachie, and Hasbrouck Heights −− said he feared the airport was "another accident away" from a catastrophic incident.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFlZUVFeXk0NSZmZ2JlbDdmN3ZxZWVFRXl5Njg2MTc3NSZ5cmlyeTdmNzE3Zjd2cWVlRUV5eTM=

17. *January 17, Department of Homeland Security* — **Homeland Security and State Departments announce initiative to keep borders secure and open.** Homeland Security Secretary Michael Chertoff and Secretary of State Condoleeza Rice announced plans to strengthen security at U.S. borders while "keeping the welcome mat out for those who want to come from overseas" at an event held at the Department of State. The joint agnda for securing borders and opening doors to those who lawfully cross our borders to work, learn, and visit includes the increased use of modern technology to establish a comprehensive enrollment network for registered, trusted travelers to the United States. "To strike the right balance between security and facilitation, we have to incorporate 21st century technology and innovation," said Secretary Chertoff in announcing plans for a new, inexpensive secure travel card for land border crossings. The new People Access Security Service (PASS) system card will be particularly useful for those in border areas who regularly cross the borders we share with Canada and Mexico as part of their daily lives.
Statement by Secretary Chertoff on Secure Borders and Open Doors In the Information Age: http://www.dhs.gov/dhspublic/interapp/speech/speech_0266.xml
Statement by Secretary of State Condoleezza Rice on Secure Borders and Open Doors: http://www.state.gov/secretary/rm/2006/59239.htm
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0838.xml

18. *December 15, Government Accountability Office* — **GAO−06−91: Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure (Report).** Congress and the President have called for various homeland security efforts to be based on risk management −− a systematic process for assessing threats and taking appropriate steps to deal with them. The Government Accountability Office (GAO) examined how three Department of Homeland Security (DHS) components were carrying out this charge: 1) the Coast Guard, which has overall responsibility for security in the nation’s ports; 2) the Office for Domestic Preparedness (ODP), which awards grants for port security projects; and 3) the Information Analysis and Infrastructure Protection Directorate (IAIP), which has responsibility for developing ways to assess risks across all types of critical infrastructure. GAO’s work focused on identifying the progress each DHS component has made on risk management and the challenges each faces in moving further. This report contains many recommendations aimed at helping the three components face their next risk management challenges. DHS, including the Coast Guard, ODP, and IAIP, generally concurred with the report and its recommendations. DHS said that all three components have

actions under way to address many of the recommendations in this report.
Highlights: http://www.gao.gov/highlights/d0691high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−91

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

19. *January 17, Billings Gazette (MT)* — **Agents round up 200 more bison for slaughter.** Government agents rounded up more than 200 Yellowstone National Park bison on Monday, January 16, and prepared to ship as many as 100 to slaughter Tuesday, January 17. The latest activity is pushing capacity limits for the bison holding facility on the northern edge of the park. As of Monday evening, about 400 bison were in the pens, where capacity for long−term holding has been pegged at around 200 in previous years. Al Nash, a park spokesperson, said park officials ought to be able to safely keep the bison until they can be taken to slaughterhouses this week. Park officials estimate that on Monday they captured 200 to 225 bison, most of them on private property north of Yellowstone. Eventually all of the bison that have been captured will be sent to slaughter, park officials said. None of the animals will be tested for brucellosis, the contagious disease that is bothering bison management. A plan signed by federal and Montana officials in 2000 allows bison to be captured and sometimes killed if the overall population meets certain requirements. The plan is intended, in part, to reduce the risk of spreading brucellosis between bison and livestock outside Yellowstone.
Brucellosis information: http://www.aphis.usda.gov/vs/nahps/brucellosis/
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2006/01/17/build/wyoming/30−bison−slaughter.inc

20. *January 17, USAgNet* — **Foot−and−mouth disease outbreak continues in Brazil.** Latest reports from the Brazilian government show that there have been no new outbreaks of foot−and−mouth disease (FMD) registered in the state of Mato Grosso do Sul. However, an outbreak was reported on a ranch in the municipality of So Sebastio da Amoreira in the state of Parana. The affected farm, which has 1,772 fattening cattle for rearing and breeding, remains under quarantine. Other suspect farms in the municipalities of Loanda, Amapora, Grandes Rios, and Maringa, continue to be under quarantine. A farm in the municipality of Bela Vista, which received animals from an outbreak in Eldorado in the State of Mato Grosso do Sul, is also under quarantine. These farms are undergoing a serological investigation for the detection of non−structural proteins, since the attempts at viral isolation were completed.
Animal−movement control is being maintained in the State of Parana, with the establishment of control posts and the application of biosafety measures. A total of 57,520 FMD−susceptible animals (26,553 cattle, 396 pigs, and 571 sheep and goats) have been culled in the state of Mato Grosso do Sul, according to a report by Jorge Caetano, director of the Department of Animal Protection in the Ministry of Agriculture, Livestock, and Food Supply.

Source: http://www.usagnet.com/story−national.cfm?Id=66&yr=2006

21. *January 17, Associated Press* — **More chronic wasting disease found in South Dakota.** Four deer and three elk tested positive for chronic wasting disease (CWD) from 2,252 samples tested since July 1 2005, according to the South Dakota Department of Game, Fish & Parks. About 3,000 samples have been collected, but not all have been tested yet. Most of the samples were submitted by hunters in Fall River, Custer, and eastern Pennington counties in the southwestern part of the state. The GF&P has found cases in 28 free−ranging deer and 12 elk from 12,032 samples tested since 1997. The latest confirmed cases were in three mule deer and an elk from Fall River County, an elk from Pennington County, a white−tailed deer from Custer County, and an elk from Wind Cave National Park.
CWD information: http://www.cwd−info.org/
Source: http://www.rapidcityjournal.com/articles/2006/01/17/news/sta te/news07.txt

22. *January 17, Kentucky Ag Connection* — **Stripe rust becoming more prevalent in Kentucky.** For years stripe rust was considered a disease that impacted wheat mostly in the Pacific Northwest. But as the disease has begun to migrate, farmers in some areas of Kentucky are seeing it impact their operations. At the recent University of Kentucky annual winter wheat meeting, Plant Pathologist Don Hershman said stripe rust has been found in the state for the past few years, with 2004−05 seeing the largest incidence. Although it had little impact on the crop, Hershman noted that its presence prompted him to present a program on the disease for the first time in his 21 years with the university. Plants susceptible to stripe rust can die if infected, and the disease can overwinter in Kentucky fields. It can affect nearly all parts of the plant. Kentucky and other areas of the country are seeing the disease because it has migrated down the west coast and into Mexico and some southern states where it now also overwinters. In addition, new races of the disease have developed that have a shorter latent period and are more tolerate to higher temperatures. Hershman said he expects stripe rust will be an issue next year.
Stripe rust information: http://www.oznet.ksu.edu/path−ext/factSheets/wheat/wheat%20s tripe%20rust.asp
Source: http://www.kentuckyagconnection.com/story−state.cfm?Id=25&yr =2006

23. *January 17, China Daily* — **Foot−and−mouth disease outbreaks reported in China.** China confirmed Monday, January 16, outbreaks of foot−and−mouth disease (FMD) in Northwest China's Ningxia Hui Autonomous Region and East China's Jiangsu Province. Two heads of cattle raised by a farmer in Xuanhe Town, Zhongwei City in the Ningxia Hui Autonomous Region showed the symptom of gum cankering, tongue blister on January 4, with one dead the next day, the Ministry of Agriculture said on its Website. The initial tests by the region's veterinary authorities indicated this a suspected Asia I strain of FMD. The National FMD Lab confirmed the case on Saturday, January 14, the ministry said. Eighty−nine heads of cattle and 110 sheep have been culled in the vicinity of the outbreak in the region to guard against the spread of the disease. In a farm in Xuzhou, Jiangsu Province, twenty cows took on the symptoms of salivation on January 11, which was diagnosed as a suspected Asia I strain of FMD by provincial veterinary authorities and confirmed by the National FMD Lab Monday, January 16.
FMD information: http://www.oie.int/eng/maladies/fiches/A_A010.HTM
Source: http://www.chinadaily.com.cn/english/doc/2006−01/17/content_512899.htm

24. *January 17, Denver Post (CO)* — **New technology to help track livestock.** Colorado is one of a handful of states −− all in the West −− that still require brand inspections of cattle, horses, and other livestock. Last year, Colorado's 65 brand inspectors traveled 1.5 million miles to do 3.8 million inspections of livestock; administered about 38,000 recorded brands; did 60,000 horse inspections; and identified owners of 80,000 head of livestock. Beginning next month, the state will provide a Website where Coloradans can register their livestock and their premises. The registration is part of the National Animal Identification System. The U.S. Department of Agriculture will make the registration mandatory in January 2008. By 2009, each animal will have a tag bearing a 15−digit number that also identifies the species group. The tags can be scanned and downloaded to a computer. While the national system is aimed at tracing an animal within 48 hours of discovering a disease, it also will provide another way of identifying animals. Colorado and 13 other states will use brand inspectors to operate the system.
Source: http://www.denverpost.com/stockshow/ci_3408564

[Return to top]

Food Sector

25. *January 17, Bloomberg* — **Singapore to lift two−year ban on U.S. beef imports.** Singapore, which suspended beef imports from the U.S. in December 2003 after a cow in Washington state tested positive for mad cow disease, will lift the ban "as soon as possible," the government said. The city−state usually bans beef imports from countries affected by bovine spongiform encephalopathy, the scientific name for mad−cow disease, for six years. It's now taking a "risk management approach" to allow beef imports from selected countries affected by the disease, the government said. Singapore "has completed its documentary and on−site review of the U.S. system for mitigation of risk," the government said in a statement distributed in Parliament Tuesday, January 17, adding that it's "ready to lift its import ban on U.S. beef and is currently finalizing operational details with U.S. officials." Before the ban in 2003, beef imports from the U.S. made up five percent of the beef in the city−state. Singapore plans to lift the ban to allow the import of de−boned beef cuts from U.S. cattle that's less than 30 months old, the government said in the statement.
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=aCaWSOkmglxc&refer=asia

26. *January 17, San Diego Union−Tribune (CA)* — **New state law bans many Mexican brands.** A California state law went into effect January 1 that bans the sale of chile−and tamarind−based candies, most of them made in Mexico, that contain high levels of lead. Lead−tainted candy is a major health threat to children under six in California, health experts said. More than 100 brands of Mexican candy are sold in small corner markets in Latino communities, out of ice cream trucks, in supermarket chains and even outside some schools. The measure, AB 21, makes selling lead−tainted candy a crime that carries a $500 fine. It gives state health inspectors greater power to confiscate tainted candy. The first of its kind in the nation, the law calls for the California Office of Environmental Health Hazard Assessment to establish the lead levels in each brand of candy. The agency will also test wrappers and containers, which often contain even more lead than the candy itself. Brands that surpass levels deemed safe will be banned until their manufacturers lower them. Officials from the state

Department of Health Services will inspect those merchants who are known to or suspected of selling brands that don't meet state standards.
Source: http://www.signonsandiego.com/news/metro/20060117−9999−1m17c andy.html

27. *January 15, BBC News* — **New way to stop food poison bacteria.** Researchers believe they may have found a novel way to disrupt bacteria that cause food poisoning. The U.S. and United Kingdom team have uncovered a previously unrecognized mechanism which bacteria use to escape the body's natural defense responses. Using this mechanism, the pathogens detect a toxic gas produced by the body and turn it into something that is harmless to evade the onslaught. The team from Georgia Institute of Technology, and the John Innes Centre looked at harmless strains of the bacterium Escherichia coli. However, they believe their findings will apply to the more harmful strains of E. coli and its close relation salmonella that cause outbreaks of food poisoning around the world. The bacterium has a protein called NorR that once activated controls the expressions of genes. These genes hold the code for an enzyme that removes the nitric oxide, allowing the bug to fend off the body's defenses. Professor Stephen Spiro explained, "It turns out that the protein NorR contains a single molecule of iron. Our study found that the nitric oxide binds to the iron, which activates the protein. "If we can interfere with the mechanism, it could lead to better antibiotics and treatments," he said.
Source: http://news.bbc.co.uk/1/hi/health/4609022.stm

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

28. *January 17, Reuters* — **Turkey confirms 21st human bird flu case.** Another child has tested positive for the H5N1 bird flu virus which has already killed four children in Turkey, the health ministry said on Tuesday, January 17. The latest case brings the total number of confirmed H5N1 cases among humans in Turkey to 21 over the past two weeks, including the four deaths. The ministry said the child had tested positive while undergoing checks in the eastern Turkish city of Erzurum. Like the four people who died, the infected child comes from the town of Dogubayazit near the Iranian border. Samples of the child's tissue have been sent to a laboratory in England for further tests, the ministry said. Prime Minister Tayyip Erdogan said on Tuesday, January 17, five patients with H5N1 had recovered and had been discharged from hospital. The four dead Turkish children are the first human bird flu fatalities outside China and Southeast Asia since the virus re−emerged in late 2003.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=global News&storyID=2006−01−17T143655Z_01_L17617634_RTRUKOC_0_US−BI RDFLU−TURKEY−CASES.xml&archived=False

29. *January 17, Agence France−Presse* — **Bird flu conference opens in China.** A two−day international donors' meeting that aims to raise 1.5 billion dollars to help fight bird flu opened

in Beijing, China. Officials from 90 countries and 25 organizations gathered Tuesday, January 17, to come up with the money needed to finance a three−year action plan. The disease, which has killed nearly 80 people mostly in East Asia since 2003, has spread to the Middle East and Europe over the past year. The conference, which is co−sponsored by China, the European Commission, and the World Bank, is aiming to assess the financing needs at country, regional, and global levels. It will invite the international community to pledge financial support and discuss how to set up mechanisms to coordinate the fight against bird flu. Funds raised will be given to needy countries in the form of grants and low−interest loans to help them strengthen surveillance. This will include the training of agriculture and health workers and strategies to better detect outbreaks and cases, and how to respond to them. Money will also be used to expand the global stockpile of anti−viral drugs and to prepare a currently non−existent human vaccine.
Source: http://news.yahoo.com/s/afp/20060117/wl_afp/healthfludonors_060117100751

30. *January 16, Georgia Institute of Technology* — **New device could enable more accurate injections.** When medics are treating trauma patients, every second counts. Yet bruises, burns, and other physical conditions often make it difficult to locate veins and administer lifesaving drugs or solutions. A team of Georgia Institute of Technology researchers is developing a handheld device that uses Doppler ultrasound technology to find veins quickly. “Depth and angle are the critical issues for vessel detection,” says project leader Michael Gray. “Even if you locate a vein at the skin’s surface, it’s still easy to miss when you try to insert a needle into the tissue below.” The Doppler effect is a phenomenon that occurs when electromagnetic and sound waves interact with a moving object, altering wavelengths and frequency. Doppler ultrasound is similar, except that acoustical waves are transmitted. Compared to static skin and tissue, blood is a moving substance, so ultrasonic waves reflected from blood vessels have different characteristics than transmitted ones, providing critical 3−D information about a vein’s location. The vein finder is composed of two parts: A reusable unit houses the electronics and signal processing components, while a disposable coupler box holds a reflector and needle guide. The needle guide is positioned parallel to the sound beam being transmitted by a transducer in the device’s reusable section.
Source: http://www.gatech.edu/news−room/release.php?id=828

31. *January 16, Agence France−Presse* — **New polio case forces Ethiopia to re−vaccinate.** Ethiopia will conduct a new round of nationwide polio vaccinations following the discovery of a new case in the country's remote southeast after two previous drives last year, the World Health Organization (WHO) said. "At least two more wide−scale campaigns will be necessary to ensure interruption of the polio virus," said William Schluter of the WHO, adding that the new case was reported after the most recent round of vaccinations meaning the disease had not been eradicated. Some 16 million Ethiopian children were vaccinated against polio last year after the first cases were reported in four years amid fears the disease was making a comeback after an outbreak in Nigeria spread to Sudan and other nations. The new drive is to kick off in mid−February and will target children under the age of five across the country. It will be followed by a second phase at an as−yet undecided date. According to WHO, the new case in East Harergue, 355 miles southeast of Addis Ababa, brings to 21 the number of people infected by the crippling and potentially fatal disease since February last year.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://news.yahoo.com/s/afp/20060116/hl_afp/healthethiopiapo

lio_060116185408;_ylt=AiK63TQuDfgh3lcLh_jRj1mJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

32. *January 12, Keep ME Current (ME)* — **Maine not prepared for public health disaster.** A legislative task force looking into Maine's homeland security needs was told at a meeting on Monday, January 9, that a lot more still needs to be done. Monday's guest panel included Dr. Dora Mills, director of the Maine Center for Disease Control and Terrance Walsch, Portland's deputy fire chief in charge of emergency services. "I can honestly say that if a pandemic breaks out tomorrow, we would be winging it," Walsch said. "We will not be ready. When we get outside of Portland into the rural areas where there's not a lot of infrastructure, I don't know what they'd do." Mills said Maine does not have a statewide public health infrastructure. She called Maine's public health preparedness, "a patchwork quilt." Since 2002 the state of Maine has received close to $32.6 million from the federal government to spend on public health preparedness. With that money, Mills said, the Maine Center for Disease Control has created a "very, very basic infrastructure." The $32 million has primarily been spent in four distinct areas, early detection, response planning, communication and training. With part of the money a new Office of Public Health Emergency Preparedness has been created within the Bureau of Health.
Source: http://www.keepmecurrent.com/Community/story.cfm?storyID=136 72

[Return to top]

Government Sector

33. *January 17, Penn State Live* — **Penn State selected for DHS National Visualization Team.** Pennsylvania State University, in University Park, has been named a Regional Visualization and Analytics Center by Pacific Northwest National Laboratory (PNNL) in Richland, WA. PNNL leads the Department of Homeland Security's (DHS) National Visualization and Analytics Center or NVAC, which is bringing academic expertise to the nation's efforts to discover information that may warn officials of a terrorist attack. The other team selections are the University of North Carolina at Charlotte, Georgia Institute of Technology, the University of Washington, and Purdue University in partnership with Indiana University School of Medicine. Stanford University was named a regional center earlier this year. DHS established the NVAC in 2004 to provide scientific guidance and coordination for the research and development of new tools and methods that DHS has identified as required for managing, visually representing, and analyzing enormous amounts of diverse data and information. Development of these visualization tools will enable analysts to more effectively identify signs of terrorist attacks in their earliest stages and ultimately to prevent terrorist activities before they can be carried out. The four core responsibilities are research and development; education; technology evaluation and implementation; and integration and coordination of research programs across government agencies.
National Visualization and Analytics Center: http://nvac.pnl.gov/
Source: http://live.psu.edu/story/15516

[Return to top]

Emergency Services Sector

34. *January 12, Federal Computer Weekly* — **Florida county builds disaster recovery applications.** When Hurricane Wilma tore through southern Florida last October, one of the biggest challenges Miami residents faced was finding gas for their vehicles. Judi Zito, Miami−Dade county's chief information officer, said employees from the information technology department developed a geographic information system application in a couple of days that merged data about gas stations with information gleaned from calls to those stations to find out if they were open and what type of gas they had available. Workers were able to enter ZIP Codes and find available gas stations in response to motorist inquiries. Officials could also map the locations of gas stations across the county to see which were located in areas that lacked electrical power and then respond by sending out portable generators. Another program called Disaster Assistance Employees, developed before last year's hurricane season, tracks county employees' skills beyond their job requirements. For example, the database can identify employees who are licensed forklift operators, speak foreign languages or have expressed an interest in assisting elderly residents in preparing for a hurricane. The application could also map employees' addresses so they can be assigned to relief activities in areas close to their homes, she said.
Source: http://fcw.com/article91952−01−12−06−Web

35. *January 12, Insurance Journal (CA)* — **Florida's Disaster Recovery Centers closing soon.** After nearly three months of serving Florida residents impacted by Hurricane Wilma, all remaining Disaster Recovery Centers (DRCs) will be ceasing operations within the next two weeks, according to the Department of Homeland Security's Federal Emergency Management Agency and Florida's State Emergency Response Team. At the peak of hurricane−relief activity, 41 DRCs were operating throughout the area affected by Wilma. As of January 9, DRCs had served more than 135,000 Florida residents. At their peak activity, DRCs across Florida served more than 5,000 residents in a single day. As more Floridians have received assistance, the number visiting the remaining centers has diminished to a small fraction of that activity. Although DRC operations will cease, U.S. Small Business Administration (SBA) workshops will continue at several former DRC locations. At the workshops, visitors can receive help in filling out disaster loan applications from the SBA. The workshops are expected to continue through the end of January and perhaps longer, if needed.
Source: http://www.insurancejournal.com/news/southeast/2006/01/11/64 009.htm

[Return to top]

Information Technology and Telecommunications Sector

36. *January 16, FrSIRT* — **AOL "YGP Picture Finder Tool" ActiveX control buffer overflow vulnerability.** A vulnerability has been identified in AOL software and AOL You've Got Pictures, which could be exploited by remote attackers to execute arbitrary commands. This is due to a buffer overflow error in the AOL YGP Picture Finder Tool ActiveX control (YGPPicFinder.dll) that does not properly handle overly long input strings, which could be exploited by remote attackers to compromise a vulnerable system by convincing a user to visit a specially crafted Webpage.

Solution: Upgrade to AOL 9.0 Optimized or AOL 9.0 Security Edition: http://downloads.channel.aol.com/
Or download and apply the hotfix: http://download.newaol.com/security/YGPClean.exe
Source: http://www.frsirt.com/english/advisories/2006/0221

37. *January 16, FrSIRT* — **Linux Kernel multiple remote and local denial of service vulnerabilities.** Multiple vulnerabilities were identified in Linux Kernel, which could be exploited by remote or local attackers to cause a denial of service. The first issue is due to an infinite loop in the "netlink_rcv_skb" [af_netlink.c] function when handling a specially crafted "nlmsg_len" value, which could be exploited by local attackers to cause a denial of service. The second flaw is due to an error in the PPTP NAT helper that does not properly calculate the offset when handling an inbound "PPTP_IN_CALL_REQUEST" packet, which could be exploited by attackers to crash a vulnerable system. The third vulnerability is due to an error in the PPTP NAT helper that does not properly calculate the offset based on the difference between two pointers to the header, which could be exploited by attackers to cause a kernel crash.
Solution: Upgrade to Linux Kernel 2.6.15.1: http://www.kernel.org/
Source: http://www.frsirt.com/english/advisories/2006/0220

38. *January 16, Network World* — **Military clamping down on security.** Lt. General Charles Croom, commander of the Joint Task Force (JTF) on Global Network Operations (GNO) and director of the Defense Information Systems Agency (DISA), last week said a sweep is underway of all Department of Defense (DoD) networks to uncover security holes amid a get−tough policy. “The attacks are coming from everywhere and they’re getting better,” said Croom in his keynote address at the DoD Cyber Crime Conference last week. The discovery of a botnet last November 5th inside DoD networks contributed to the decision to clamp down security. So far, the results are troubling. “Almost 20 percent of our accounts are unauthorized or had expired,” Croom said, noting that military personnel tend to move every two or three years and accounts are sometimes left open. The exact tally of improper accounts won’t be known until March, he said. The biggest changes to come may be in the next six months as the JTF−GNO, the organization set up to centralize decisions about security and operations in the Army, Navy, Air Force and Marines, evaluates a possible redesign of its two primary global IP−based military networks.
Source: http://www.networkworld.com/news/2006/011606−military−securi ty.html

39. *January 16, VNUNet* — **Windows 2000/XP fall through Wi−Fi flaw.** Hackers have exposed details of a previously undocumented flaw in Microsoft's handling of Wi−Fi which affects users of Windows 2000 and XP. The vulnerability was detailed at the Shmoocon hackers conference in Washington, DC, by self−confessed hacker Mark Loveless, (a.k.a. Simple Nomad), a senior security researcher for Vernier Threat Labs. Loveless explained that the issue centers on the way in which the operating systems look for wireless networks during start−up. When a Wi−Fi equipped laptop starts up using Windows 2000 or XP it immediately starts scanning for wireless networks. If none is found it sets up an ad hoc link using the name of the last wireless network accessed. If a hacker was aware of the last used network ID, for example knowing the name of a corporate Wi−Fi network address, it could be used to establish a direct local link with the Windows PC offering access to all local drives. However, the problem only arises if the target machine is not running a firewall. One of the changes in Windows XP SP2 turns the

built−in firewall on by default.
Source: http://www.vnunet.com/vnunet/news/2148609/microsoft−wi−flaw− found

40. *January 16, Reuters* — **Spain arrests hacker after breach at U.S. Navy base.** Spain's Civil Guard said on Monday, January 16, they had arrested a man who hacked into a U.S. Department of Defense computer, breaching security at a U.S. naval base in California. The man was part of a group of hackers which attacked more than 100 computer systems, including one at the U.S. Navy's Point Loma base in San Diego where nuclear submarines are maintained in dry docks. U.S. security services found someone had illegally accessed the computer and subsequently traced the link to Spain. Spanish authorities pinpointed the group in the southern city of Malaga and arrested one man. Many of the group were students though all were over 18. "They did it for the challenge, there's no implication of terrorism," a Civil Guard spokesperson said, adding that the man would face unspecified charges. The Guard did not say when the arrests or the hacking took place.
Source: http://today.reuters.com/news/newsArticleSearch.aspx?storyID=210818+16−Jan−2006+RTRS&srch=hacker

41. *January 16, Help Net Security* — **Number of "classic" viruses dropped dramatically in 2005.** According to data released by PandaLabs, less than one percent of the new threats detected in 2005 were viruses, whereas threats like Trojans and worms still had a significant presence compared to the previous year. “Viruses, described as threats that add their code to other executable files in order to carry out their malicious actions, have reached rock bottom this year,” explains Luis Corrons, director of PandaLabs. “The aim of creators of this type of threat is usually fame. However, legislation against computer crime in many countries worldwide has led to a dramatic drop in the number of new specimens of this type. Now, almost nobody runs the risk if it does not lead to financial gain.” Of the new threats detected by PandaLabs in 2005, 42 percent were Trojans, 26 percent were bots, 11 percent were backdoor Trojans, eight percent were dialers, six percent were worms and three percent were types of adware/spyware.
Source: http://www.net−security.org/press.php?id=3761

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.

Malicious Website Exploiting Sun Java Plug−in Vulnerability:

US−CERT is aware of an active malicious website that exploits a vulnerability in the Sun Java JRE. The initial report led US−CERT to believe the website was exploiting VU#974188. After further analysis, it was determined that the actual vulnerability being exploited was VU#760344. This vulnerability allows a Java Applet to bypass java security settings. Once these checks are bypassed, a remote attacker may be able to exploit this vulnerability to execute arbitrary code on the host machine. More information about these vulnerabilities can be found in the following URL:

VU#760344 Sun Java Plug−in fails to restrict access to private Java packages:
http://www.kb.cert.org/vuls/id/760344

VU#974188 Sun Java Runtime Environment "reflection" API privilege elevation vulnerabilities: http://www.kb.cert.org/vuls/id/974188

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 139 (netbios−ssn), 27015 (halflife), 135 (epmap), 54000 (−−−), 25 (smtp), 7008 (afs3−update), 80 (www) 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