Department of Homeland Security Daily Open Source Infrastructure Report for 30 January 2006

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

Daily Highlights

- The Deseret News reports agents with the FBI, U.S. Postal Service, U.S. Secret Service, and Utah law enforcement have announced the breakup of a major identity−theft ring that involved more than 25,000 checks and hundreds of victims. (See item 9)
- The Associated Press reports authorities have discovered more than two tons of marijuana in a cross−border tunnel that began near the Tijuana airport and ended inside a warehouse in a San Diego neighborhood near the border. (See item 16)

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 28, Associated Press* — **Nuclear power plant shutting down to check malfunction.** The operators of the Oyster Creek nuclear power in Lacey Township, NJ, plant intend to shut down as soon as weather permits so they can investigate two broken pumps used to cool its reactor. One of the five large pumps, which circulate cool water through the reactor, shut down just before 9 a.m. EST Wednesday, January 25; the other shut down last summer. The malfunction is believed to be caused by a short in power to pump ground cables, Neil Sheehan, a spokesperson for the Nuclear Regulatory Commission, said. The 630−megawatt plant in Lacey Township is the oldest commercial nuclear power plant in the United States. The plant

can operate at full power with one pump inoperable, but with two down it was running at about 53 percent power last week. Pete Resler, a spokesperson for AmerGen, the energy company that operates Oyster Creek, said that he would not disclose when the plant is shutting down because it could impact energy market prices. Plant operators will slowly shut the plant down so that the discharge temperature drops by about one degree an hour.
Source: http://1010wins.com/topstories/local_story_028220413.html

2. *January 28, Associated Press* — **Judge orders Aquila to tear down power plant.** A Cass County, MO, judge on Friday, January 27, gave utility Aquila Inc. until May 31 to begin tearing down a $140 million power plant that went up last summer without county approval. Circuit Judge Joseph Dandurand also told the company to cease plant operation immediately. Dandurand rejected calls from Cass County attorneys that he order the power plant dismantled immediately. He said he was willing to give the Kansas City−based company time to ask the Missouri Public Service Commission to intervene and save the plant, built near Peculiar. The judge said he thought tearing down the plant would be wasteful, but he did admonish Aquila officials for what he called their "arrogance" and "disregard for the law." Aquila began operating the 315−megawatt South Harper power plant in June, saying a state−issued "certificate of need" meant it didn't need to receive zoning approvals from county officials.
Source: http://www.newstribune.com/articles/2006/01/28/news_state/01_28060042.txt

3. *January 28, Agence France−Presse* — **OPEC sees no emergency in Iranian nuclear crisis.** The Organization of the Petroleum Exporting Countries (OPEC) sees no need to adopt emergency measures for oil production due to the crisis between Iran and the Western powers over Tehran's nuclear program, says OPEC's president, Edmund Daukoru. Speaking in Vienna, Austria ahead of an OPEC meeting, Daukoru said, "I don't want to treat the Iran case as some kind of emergency that would call for an emergency response." A key issue in talks between the 11 nations of the cartel will be Iran's call to cut production. Iran, the world's fourth largest oil producer, has warned of higher oil prices and threatened to suspend exports if the International Atomic Energy Agency, refers Iran to the UN Security Council for sanctions over its nuclear ambitions. Acting OPEC secretary general Mohammed Barkindo said that OPEC, which supplies more than a third of the world's oil, would pump more if Iran cuts its output. Oil markets are also jittery about growing instability in Nigeria with respect to attacks on foreign oil companies, which has crimped the No. 6 oil producer's production.
Source: http://news.yahoo.com/s/afp/20060128/bs_afp/opecenergyoilira n_060128205050

4. *January 27, Rutland Herald (VT)* — **Towns agree to vote on nuclear escape planning.** Town meeting articles calling for increased evacuation readiness in case of a nuclear emergency will appear on the ballots in five towns near Vermont Yankee nuclear power plant this year. Residents in Brattleboro, Dummerston, Guilford, Halifax, and Marlboro will be asked if state legislators should appropriate more funds for local emergency planning, including increased shelter room, full siren alerts, and more evacuation drills. Members of Nuclear Free Vermont said they do not want to see a repeat of Federal Emergency Management Agency's slow and tepid response to Hurricane Katrina last fall. Entergy Vermont Nuclear, the parent company of Vermont Yankee, funds local evacuation planning. The questions calls on Vermont Emergency Management to secure shelter and decontamination units for the whole population within a 10−mile radius of Vermont Yankee, and not 20 percent as it does now. It also asks for emergency sirens, phone warning systems and evacuation drills for schools, hospitals and elder

and child−care facilities in the zone. Barbara Farr, the director of Vermont Emergency Management, said "We don't plan just for the evacuation of 20 percent of the people...That's the amount that is expected to evacuate to the designated center."
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20060127/NEWS/601270352/1003

5. *January 26, National Public Radio* — **Study backs ethanol as gasoline substitute.** About one out of every 40 cars and trucks in the U.S. can now run on a commercial mix of gasoline and ethanol. But does ethanol really reduce dependence on other forms of energy, such as oil or coal? CITGO gas station manager Wang Kan who sells E85 fuel −− 85 percent ethanol and 15 percent gas −− in Annapolis, MD, says when gas prices were high last year, 10 times as many people bought ethanol. Did that switch reduce America's consumption of oil and other fuels? It all depends on how you add up the amount of energy needed to make ethanol. Dan Kammen, a physicist and energy expert at the University of California at Berkeley, asks "Do you include the energy to build the factory, the tractors?...it boils down to a critical thing: Do we do better from a national security perspective...by burning gasoline or by growing a biofuel and putting that in our tank?" Kammen and his colleagues at Berkeley think the nation does benefit from using biofuels. However, David Pimentel, an agriculture scientist at Cornell University, disagrees. He says it takes 70 percent more energy to make gallon of ethanol than it gives off.
Study: http://www.sciencemag.org/cgi/content/full/311/5760/506
Source: http://www.npr.org/templates/story/story.php?storyId=5173420 &ft=1&f=1007

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

6. *January 27, Aviation Week* — **Supplemental favors Army again, analysts say.** The recently passed $50 billion U.S. military supplemental legislation will continue to provide incremental growth to the overall defense budget and top−line for defense contractors, especially companies with heavy exposure to the Army, according to Peter Arment of JSA Research Inc. The Army continues to receive strong supplemental funds, with 63 percent of the total supplemental, he said Wednesday, January 25. More than $9 billion of the supplemental has been allocated to procurement, with 49 percent going to the Army. Specifically for the Army, $860 million is being allocated for tracked combat vehicles and related weapons and $273 million for ammunition, likely small caliber, while $232 million goes to Army aircraft, probably mostly helicopters, Arment said. James McAleese of McAleese & Associates PC believes the Army will continue to receive "strong" funding in the next supplemental spending request this spring. McAleese said he expects the spring request to be for $50 billion. According to McAleese, the Navy received almost 13 percent of the last supplemental while the Air Force received six percent. Supplemental funds across the Department of Defense account for 18 percent of the total. His calculations do not include military construction and research, development, testing

and evaluation allocations.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/ARM01276.xml

7. *January 27, Seattle Times (WA)* — **Pentagon tanker study leaves time frame in air.** After a year's wait, the Pentagon's study on options for replacing the Air Force's aging refueling tankers was presented in several closed briefings Thursday, January 26, to select members of Congress. The good news, said Rep. Norm Dicks (D−WA) was that it focuses on adapting medium−to−large commercial planes, opening the door for Boeing and Airbus to compete for the Pentagon project. But a new tanker contract could still be months away. "The study made no definitive conclusions about the timing of the tanker replacement, because it was primarily an analysis of cost−effectiveness," said Dicks in a news release. Researched largely by the Rand Corp., the Pentagon study narrowed the possibilities to six airframes: Boeing's 767, 777, 787 and 747, as well as the Airbus 330 and 340. Dicks said it did not specifically suggest a combination tanker−cargo plane or a tanker−only aircraft. The study, called the Analysis of Alternatives, recommends the Pentagon weigh other factors besides economics to determine how quickly to solicit bids, he said. This was important, said Dicks, a member of the House Defense Appropriations Committee and a strong supporter of Boeing. The average age of the existing tankers is 45 years, he said.
Source: http://seattletimes.nwsource.com/html/businesstechnology/2002765131_boeingtanker27.html

8. *January 26, Defense News* — **Lockheed, Boeing, Northrop top Pentagon's 2005 Contractors Report.** The Pentagon let out contracts worth $270 billion during the financial year 2005, about $39 billion more than in 2004, according to the Department of Defense's annual Top Contractors Report, released Thursday, January 26. Lockheed Martin continued to be the largest Pentagon contractor, bagging $19.4 billion worth of business, followed by Boeing with $18.3 billion and Northrop Grumman with $13.5 billion. The top three positions remained unchanged from the previous year. But UK−based BAE Systems −− including its U.S. arm, BAE Systems North America −− moved up from the 12th spot in 2004 to No. 7 in 2005, mostly on the strength of the company's acquisition of United Defense Industries, the U.S. land armaments maker whose products include Bradley fighting vehicles and 155mm field artillery. BAE's Pentagon contracts added up to $5.6 billion in 2005. The Pentagon spent most of its contract dollars −− about $126 billion −− buying "supplies" or weapon systems, about $105 billion on "other services" and $37 billion on research and development activities.
Source: http://www.defensenews.com/story.php?F=1493801&C=america

[Return to top]

Banking and Finance Sector

9. *January 28, Deseret News (UT)* — **Six arrested in breakup of identity theft ring.** Federal agents have announced the breakup of what they call a major identity−theft ring that involved more than 25,000 checks and hundreds of victims. Agents with the FBI, U.S. Postal Service, U.S. Secret Service, and local law enforcement said the check−fraud ring was driven by the need to buy methamphetamine for its drug−addicted members. During a press conference Friday, January 27, U.S. District Attorney for Utah Paul Warner announced the indictment of

six Salt Lake City residents who are accused of running a counterfeit check−cashing ring that resulted in more than $375,000 in losses. "We're really striking at the heart of a major operation here in Utah," Warner said. Salt Lake FBI Special Agent−in−Charge Tim Fuhrman said the group created fake identification and checks and used a network of runners to cash those checks at various local banks and credit unions. Agents said that some members of the ring had ties to local white supremacist organizations, but their common goal was to feed their methamphetamine addictions. The group faces federal felony charges, including conspiracies to commit identity fraud, bank fraud, racketeering, and aggravated identity theft.
Source: http://deseretnews.com/dn/view/0,1249,635179848,00.html

10. *January 28, Duluth News Tribune (MN)* — **Stolen computer contained 12,000 students' personal information.** The College of St. Scholastica in Duluth, MN, is warning about 12,000 current and former students that they could be the victims of identity theft. The warning comes after the theft and recovery of a computer that once contained data files with names and Social Security numbers. The college notified students, faculty, and staff members of the theft via e−mail Friday morning, January 27. It also mailed letters to past students. Patrick Flattery, vice president for finance, wrote in the letter, "We have no evidence that would lead us to believe any personal information was retrieved or used inappropriately...However, between the time of the theft and the computer's recovery, an unauthorized individual could have accessed your personal information." The computer was taken from a locked office in the college's Information Technology Department on or shortly before Saturday, December 24. It was recovered Thursday, December 29. "A suspect has admitted to the theft and denies retrieving or making use of any personal data on the computer," college spokesperson Bob Ashenmacher said. "However, it's possible someone could have accessed the information."
Source: http://www.duluthsuperior.com/mld/duluthsuperior/news/local/13734979.htm?source=rss&channel=duluthsuperior_local

11. *January 27, Financial Times (UK)* — **FBI chief urges sharing of information to combat hackers.** The director of the FBI, Robert Mueller, has urged the world's law enforcement agencies to introduce a rapid system of exchanging information to battle computer security breaches and fraud. A survey by Swiss Re, a reinsurance group, showed that companies across the developed world rank computer−based risks as their main concern, well ahead of other worries such as corporate governance and natural disasters. Law enforcement agencies across the world struggle to track down and punish criminals whose use of the Internet means they often have a global reach. Yet card operators are proving increasingly successful at limiting the amount of fraudulent activity. Christopher Rodrigues, chief executive of Visa International, said the amounts lost to fraud on Visa's network had fallen to seven cents out of every $1,000 spent, down from 14 cents in the past several years. However, the growth in credit card transactions had prompted the absolute level of losses to increase. Rodrigues said fraud and identity theft had been exacerbated by the growth of electronic commerce, which meant consumers relied on banks and retailers to keep their information safe. Most banks have a regulatory obligation to look after data, but these regulations do not extend to retailers.
Source: http://news.ft.com/cms/s/015645c4−8ed9−11da−b752−0000779e234 0.html

12. *January 26, KIROTV−7 (WA)* — **Alleged Washington identity theft ring discovered.** A couple has been accused of running a $1 million identity theft ring near Tacoma, WA. The couple allegedly used South Sound, WA teens to steal as much as $1 million from more than

100 bank and credit union customers. Some of the teens sold their parents' checking account numbers to the ring. Those parents lost as much as $20,000. The News Tribune of Tacoma said investigators believe the ring has been operating since 2002, and is among the most sophisticated they have seen, said deputy prosecuting attorney Lisa Wagner. She said, "They were generating false checks and ID cards...They had to have knowledge of the banking system and how to create checks." Detective Glenda Nissen said charges against three others are pending and another four to six people may face charges.
Source: http://www.kirotv.com/news/6471128/detail.html?rss=sea&psp=n ews

[Return to top]

Transportation and Border Security Sector

13. *January 28, New York Times* — **After crash, safety board warns pilots on reversers.** Giving a strong indication of why a Southwest Airlines plane ran off the end of a runway at Midway Airport in Chicago on December 8, plowed through a fence and killed a boy in a passing car, the National Transportation Safety Board said Friday, January 27, that pilots should never assume the successful use of their thrust reversers, which are used after touchdown to turn around the jet blast and slow the plane. Airline dispatchers, who plan and monitor flights, make sure before departure that planes will be able to land safely at their destinations and are not allowed to assume that the thrust reversers will work. En route, when pilots know the weather at their destination and which runway they will be using, they usually perform a second calculation. Southwest pilots carry laptops that run Boeing software to calculate stopping distance. The union for Southwest pilots sent its members a letter on Monday, January 23, recommending that they trick the laptop by listing the thrust reversers as broken when calculating stopping distance. The board made an urgent recommendation to the Federal Aviation Administration to forbid pilots to take the thrust reversers into account when calculating stopping distance.
Source: http://www.nytimes.com/2006/01/28/national/28crash.html?_r=1 &pagewanted=all

14. *January 27, Courier−Journal (KY)* — **Barge leaking diesel, asphalt; Ohio River closed to commercial traffic.** A barge was lodged against the Kentucky & Indiana (K & I) Railroad Bridge Thursday night, January 26, leaking hot asphalt and diesel fuel into the Ohio River. Authorities said the situation was unstable throughout the night. The river was closed to commercial traffic Thursday night until the situation was resolved. It was one of three barges that broke loose from their tow Thursday afternoon near McAlpine Locks, with two going over the dam's spillway. The Sherman Minton Bridge was closed briefly about 7:30 p.m. EST, after the leaking barge shifted, prompting fears it might smash into the bridge's supports if it got past the K & I Railroad Bridge. But the U.S. Coast Guard reopened the Sherman Minton minutes later, when it appeared the barge was sinking. Tests showed the concentration of diesel to be one part per million. Levels would have to reach 200 or 300 parts per million to cause health concerns, Dr. Matt Zahn, medical director of the Louisville Metro Health Department. The barge carried 15,000 gallons of diesel fuel used to power heaters that keep the asphalt at a constant liquid temperature.
Source: http://www.courier−journal.com/apps/pbcs.dll/article?AID=/20 060127/NEWS01/601270457/1008/NEWS01

15. *January 27, Washington Post* — **United to take Dulles gates.** United Airlines has a deal with defunct Independence Air to take over the 35 gates that Independence leased in Washington Dulles International Airport's Concourse A, which is used for short commuter flights. The $4.3 million agreement would further United's planned expansion in the Washington, DC market, enabling the Elk Grove Township, IL−based carrier to feed more passengers from commuter flights onto longer−haul West Coast and international flights. The deal is subject to approval by the U.S. Bankruptcy Court in Delaware. UAL Corp. Chairman Glenn F. Tilton said this week that he plans to make United's East Coast hub at Dulles a major gateway to Europe, Latin America and South Africa. United also is lining up partners: It recently signed a code−sharing agreement with South African Airways, which operates a one−stop flight from Dulles to Johannesburg. United's bid for the new gates came in an auction Flyi is holding for its assets. Independence stopped flying on January 5, citing record fuel prices and unrelenting competition, including that from United.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/26/AR2006012602004.html?sub=AR

16. *January 26, Associated Press* — **Two tons of marijuana found in cross−border tunnel.** Authorities said they discovered more than two tons of marijuana in a cross−border tunnel that began near the Tijuana airport and ended inside a warehouse on the U.S. side. The 2,400−foot long passageway is longer than most of the 21 cross−border tunnels that have been discovered since authorities began keeping track after the September 11 attacks, U.S. Immigration and Customs Enforcement officials said. John Fernandes, special agent in charge of the Drug Enforcement Administration's San Diego office, said he suspected the tunnel was the work of Tijuana's Arellano−Felix drug smuggling syndicate or another well−known drug cartel. The tunnel's discovery prompted the U.S. Attorney's office in San Diego to open a criminal investigation, said Lauren Mack, a spokesperson for U.S. Immigration and Customs Enforcement. The tunnel exited into a large, two−story white cinderblock warehouse in an industrial San Diego neighborhood near the border. Mexican authorities found the entrance about 100 yards south of the border on Tuesday, January 24, and officers on the U.S. side found the exit Wednesday, January 25. The tunnel was about five feet wide and high enough for an adult to stand inside, had a cement floor, and lights mounted on one of the hard soil walls.
Source: http://www.usatoday.com/news/nation/2006−01−26−drug−tunnel_x .htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

17. *January 29, Associated Press* — **Brucellosis testing, elk slaughter to start.** The Wyoming Department of Game and Fish expects to trap elk at the Muddy Creek feedground near Pinedale on Sunday, January 29, for its test−and−slaughter program aimed at reducing brucellosis. The department will capture as many as 300 elk to test the females for brucellosis. Those that test

positive will be slaughtered. Eric Keszler, a spokesperson for the Wyoming Game and Fish Department, said Saturday, January 28, the trapping will occur early Sunday. The department has built a large enclosure in the area. Governor Dave Freudenthal's Brucellosis Coordination Team has recommended the test−and−slaughter program as part of its plan to regain Wyoming's brucellosis−free status. Without that status, cattle exported from the state must undergo costly testing requirements. Brucellosis, a bacterial disease, can cause pregnant elk, cattle, and bison to abort their fetuses. Wyoming lost its brucellosis−free status after a cattle herd near Pinedale and other cattle herds in western Wyoming tested positive for the disease in 2003 and 2004.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2006/01/29/build/wyoming/65−elk.inc

18. *January 26, Daily Sentinel (CO)* — **Deer hit by outbreak of conjunctivitis.** An outbreak of conjunctivitis in deer herds in northwest Colorado has resulted in nearly 100 deer being killed by the Colorado Division of Wildlife. Conjunctivitis, commonly known as pinkeye, is a highly infectious disease found occasionally in wildlife, domestic livestock, and humans. However, in the latter two species the disease can be spotted early and treated successfully. When pinkeye hits wildlife, however, it's often not noticed until it's too advanced to treat. "This time of year, the deer are typically concentrated in remote areas where people can't see them," said Bill deVergie, Meeker area manager for the Division of Wildlife. "We really don't know how widespread it is in those areas we are experiencing it." Field officers have killed more than 75 conjunctivitis−infected deer this winter, 80 percent of them young bucks, deVergie said.
Source: http://www.gjsentinel.com/news/content/news/stories/2006/01/26/1_27_Deer_pinkeye.html

[Return to top]

Food Sector

19. *January 27, Animal and Plant Health Inspection Service* — **Argentina added to list of regions considered free of exotic Newcastle disease.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is amending import regulations regarding live poultry and poultry products to add Argentina to the list of regions considered free of exotic Newcastle disease (END). The requirements state that all shipments of poultry and poultry products from Argentina must be accompanied by certification from a full−time, salaried veterinary officer and must be presented to an authorized inspector at the port of arrival in the U.S. The certification must state that live poultry and poultry products did not come in contact with poultry or products from any region where END is known to still exist; have not lived in a region where END is considered to exist; have not been transported through a region where END is considered to exist unless they were moved directly through the region in a sealed container and the seal was intact upon arrival at the point of destination; and all processed poultry meat and or poultry products were processed in region known to be END−free, in a federally inspected processing plant under the direct supervision of a full−time, salaried veterinarian of the Argentine government.
Source: http://www.aphis.usda.gov/newsroom/content/2006/01/aendfree. shtml

20.

January 26, Science — **Prions in skeletal muscles of deer with chronic wasting disease.** The emergence of chronic wasting disease (CWD) of deer and elk in an increasingly wide geographic area and the interspecies transmission of bovine spongiform encephalopathy (BSE) to humans in the form of variant Creutzfeldt Jakob disease (vCJD) have raised concerns about the zoonotic potential of CWD. Since meat consumption is the most likely means of exposure, it is of considerable importance to determine whether skeletal muscle of diseased cervids contains prion infectivity. Here bioassays in transgenic mice expressing cervid prion protein revealed the presence of infectious prions in skeletal muscles of CWD−infected deer demonstrating that humans consuming or handling meat from CWD−infected deer are at risk to prion exposure.
Source: http://www.sciencemag.org/cgi/content/abstract/1122864v1

21. *January 26, U.S. Food and Drug Administration* — **U.S. Food and Drug Administration seeks injunction against shellfish processor.** The U.S. Food and Drug Administration (FDA) is seeking a permanent injunction against Pacific Shellfish, Inc., a seafood processor located in San Diego, CA, and its president. An injunction is a court order to stop a firm from manufacturing, distributing, processing, or shipping a product. The government's complaint, filed on January 24, 2006 by the U.S. Department of Justice in the U.S. District Court for the Southern District of California, charges the defendants with violating the Federal Food, Drug, and Cosmetic Act by permitting ready−to−eat fish held and processed in Pacific Shellfish's facility to become contaminated. According to the complaint, recent FDA inspections in 2004 and 2005 revealed the presence of Listeria monocytogenes, a disease−causing bacterium, on Pacific Shellfish's processing equipment and fish products. Inspections since 2001 have also documented persistent unsanitary conditions at the facility. FDA issued a letter to the firm on December 8, 2004, after an inspection revealed unsanitary conditions and contamination with Listeria. Although the firm promised to correct its deficiencies, a 2005 inspection found that a persistent strain of Listeria remained and the firm had not implemented all of the promised corrections. Listeria monocytogenesis the causal agent of listeriosis, a disease that can be serious, even fatal.
Source: http://www.fda.gov/bbs/topics/news/2006/NEW01303.html

22. *January 25, U.S. Food and Drug Administration* — **Tortillas recalled.** Del Rey Tortilleria, Inc. of Chicago, IL, is recalling FLOUR TORTILLAS because government officials have associated consumption of the flour tortillas with a series of health symptoms among individuals who complained of stomach pains, vomiting, diarrhea, nausea, and headaches. These reported symptoms typically occurred very soon after consuming the flour tortillas and resolved within one day. There does not appear to be any long−term adverse health effects. The product was distributed nationwide through food distributors and grocery stores. The affected products are all sizes and types of FLOUR TORTILLAS with the brand name Del Ray and use−by date codes of March 06, 2006 or earlier. They may be labeled as White Flour Tortillas; Tortillas de Harina; Burritos 2, 3 and 4; or Fajita 8" size. Federal and State officials have determined an association between consumption of these flour tortillas with a series of foodborne illness outbreaks, but a causative agent is still being investigated. Although the company is not certain that is products caused these symptoms, it is nevertheless recalling the product as a precaution while its investigation is continuing.
Source: http://www.fda.gov/oc/po/firmrecalls/delrey01_06.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

23. *January 29, Agence France−Presse* — **H5N1 strain of bird flu found in Cyprus.** The European Commission has said the deadly H5N1 strain of bird flu was detected in samples from the Turkish Cypriot north of Cyprus, the first ever cases to be found on the island. Cyprus lies some 45 miles from the southern coast of Turkey, where four people have died from H5N1. The Turkish cases were the first human deaths from avian influenza outside Asia. The European Union's executive arm is expected to announce soon whether the positive samples, which were tested by a British laboratory, came from two domestic poultry birds that were diagnosed with bird flu on Wednesday, January 25. The ill birds were detected on Monday, January 23, in a village near Famagusta on the eastern coast of Cyprus. Since then the Turkish Cypriot authorities have slaughtered around 1,500 poultry birds in the village. Strict checks have now been introduced at crossings between the Turkish Cypriot north of the island and the Greek Cypriot south.
Source: http://news.yahoo.com/s/afp/20060129/hl_afp/healthflucypruse u_060129134906

24. *January 28, Agence France−Presse* — **France drafts troops to fight disease in Indian Ocean island.** France is drafting 400 extra troops into the fight against mosquitoes that are spreading a crippling and incurable disease across the Indian Ocean island of Reunion, Health Minister Xavier Bertrand said. Bertrand was speaking after talks with Prime Minister Dominique de Villepin and Overseas Territories Minister Francois Baroin as the number of reported cases of the disease known as chikungunya hit 30,000 since it broke out last March. Baroin said he was also flying Monday, January 30, to Reunion together with dozens of health experts and extra equipment to strengthen the care of sufferers. The 400 troops, already stationed on the island, would add to the more than 1,500 people engaged in the campaign to eliminate the mosquitoes. Villepin's office said Saturday, January 28, that Paris would be stepping up efforts to combat the disease in liaison with the World Health Organization.
Chikungunya information: http://www.phac−aspc.gc.ca/msds−ftss/msds172e.html
Source: http://news.yahoo.com/s/afp/20060128/hl_afp/francereunionhealth_060128195748;_ylt=AhtbZt_mtl8FfEvmKxfXqbiJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

25. *January 28, Reuters* — **United Nations may use flu−casters if pandemic hits.** The United Nations (UN) is considering using flu−casters, modeled on television weather forecasters, to publicize vital information if a global flu pandemic strikes. They could broadcast latest developments from emergency−response facilities at the UN's World Health Organization (WHO) in Geneva, Switzerland, according to David Nabarro, the UN's top influenza coordinator. "The flu−casters would draw out the maps and keep people engaged at regular intervals beaming it from the WHO bunker," Nabarro told Reuters in an interview at the World

Economic Forum in Davos, Switzerland. The WHO's Geneva bunker, a five million dollar facility built in a former cinema, is the world's nerve−center for tracking deadly diseases. The room will become a global command center if the H5N1 bird flu virus, which has killed at least 83 people in Asia since 2003, mutates into a form which spreads easily among humans and sparks a flu pandemic. The screen−filled bunker could link the flu−casters with TV networks via satellite feeds.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=worldNews&storyID=2006−01−28T231834Z_01_L28274955_RTRUKOC_0_UK−DAVOS−BIRDFLU.xml&archived=False

26. *January 26, Associated Press* — **Scientists identify bird flu genes, genomes.** Scientists who have made a big leap in unraveling the genetic code of bird flu viruses along the way found a new clue that may help explain why the H5N1 strain is so deadly. St. Jude Children's Research Hospital in Memphis, TN, is home to a remarkable viral library, samples of about 11,000 influenza viruses that Robert Webster has gathered from around the world since 1976. They're not just flu viruses that have infected people over the years, but ones from pigs and other animals −− including about 7,000 bird flu viruses, gathered from poultry, ducks, gulls, and other flocks. Thursday, January 26, St. Jude researchers reported that they have completed the first large genetic analysis of more than 300 of these bird flu viruses. They identified 2,196 bird flu genes and 160 complete genomes, doubling the amount of genetic information available for scientists to study how these viruses evolve and spread over time. Simply having that new trove of gene information −− posted in a public genetic database so that any scientist can mine it −− in itself is a huge step, said Maria Giovanni of the National Institutes of Health, which has launched a major project to map influenza genomes.
Abstract: http://www.sciencemag.org/cgi/content/abstract/1121586v1
Source: http://www.usatoday.com/news/health/2006−01−26−birdflueresearch_x.htm?POE=NEWISVA

27. *January 26, Associated Press* — **Mayors asked to prepare for bird flu.** Many of the nation's mayors said Thursday, January 26, it's a challenge making bird flu preparation. Still, they say they're making preparations. If a global pandemic does strike, the nation's cities and towns cannot expect the federal government to save them, members of The United States Conference of Mayors were told. "Any community that fails to prepare −− with the expectation that the federal government can or will offer a lifeline −− will be tragically wrong," said Alex Azar, deputy secretary for the U.S. Department of Health and Human Services. Azar told the mayors they should plan for a worst−case scenario, the kind that occurred in 1918. Using that scenario, about 30 percent of their community would become ill, and half of those people would need significant medical attention. About two percent of the community would die. "If you run a small business where you employ 100 people, or you're a principal of a school with 100 faculty members, you need to plan on how you would operate if 30 to 40 of your people are absent from your work force" during each wave of a pandemic, he said.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/n/a/2006/01/26/national/w125147S12.DTL

28. *January 10, PLoS Medicine* — **Sequence−based early warning system for the detection of MRSA outbreaks in hospitals.** The detection of methicillin−resistant Staphylococcus aureus (MRSA) usually requires the implementation of often rigorous infection−control measures.

Prompt identification of an MRSA epidemic is crucial for the control of an outbreak. Researchers evaluated various early warning algorithms for the detection of an MRSA cluster. Between 1998 and 2003, 557 non−replicate MRSA strains were collected from staff and patients admitted to a German tertiary−care university hospital. The repeat region of the S. aureus protein A (spa) gene in each of these strains was sequenced. Using epidemiological and typing information for the period 1998–2002 as reference data, clusters in 2003 were determined by temporal−scan test statistics. Various early warning algorithms (frequency, clonal, and infection control professionals [ICP] alerts) were tested in a prospective analysis for the year 2003. A total of 549 of 557 MRSA were typeable using spa sequencing. When analyzed using scan test statistics, 42 out of 175 MRSA in 2003 formed 13 significant clusters. These clusters were used as the "gold standard" to evaluate the various algorithms. Clonal alerts (spa typing and epidemiological data) were 100 percent sensitive and 95.2 percent specific. Frequency (epidemiological data only) and ICP alerts were 100 percent and 62.1 percent sensitive and 47.2 percent and 97.3 percent specific, respectively. Both methods exhibited a positive predictive value above 80 percent.
Source: http://medicine.plosjournals.org/perlserv/?request=get−document&doi=10.1371/journal.pmed.0030033

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

29. *January 27, Jacksonville Daily Record (FL)* — **Fire−Rescue convention held in Florida.** Hundreds of vendors and thousands of fire and rescue personnel from around the nation gathered late last week for the Fire−Rescue East 2006 Conference and Exposition at the Osborn Center in Jacksonville, FL. The four−day conference brought more than 15,000 people to the city. Fire−Rescue East draws from more than 36 states and Canada. With the participation of national fire and rescue organizations, this event is one of the largest fire and emergency services educational events and expositions in the Southeast, according to the Foundation of Florida Fire Chiefs Association. Last year more than 11,000 people came through the city for the conference, according to Jennifer McFee, director of communications for Jacksonville and the Beaches Convention & Visitors Bureau. The event will be held in Jacksonville until 2008, after which the show will go into negotiations to stay in Jacksonville or move to another location with more convention space. The conference and exposition hosts people who manufacture and produce equipment used for fire truck and emergency teams, as well as the administrative personnel that make up those departments. It's also an opportunity for fire personnel and emergency medical technicians to keep their certifications current.
Source: http://www.jaxdailyrecord.com/showstory.php?Story_id=44452

30. *January 27, Journal−Standard (IL)* — **Federal funds secured for emergency communication in Illinois.** Congressman Don Manzullo (R−IL) announced last week that he

has secured $170,000 in federal money to help fund a new program designed to improve regional communications in Illinois between police and fire agencies in the event of a terrorist attack or natural disaster. The funding, which was secured as a federal earmark through the Congressional appropriations process, will help kick off the initiative known as the Prairie Shield Regional Alliance, which is a consortium of first responders from McHenry, Boone, Winnebago, Stephenson, Ogle, and DeKalb counties. The goal of the consortium is to allow police, fire and other emergency response teams in the region to communicate on a "voice, data, and video platform with interoperable capability." "This is enough to get the project started," Manzullo spokesperson Rich Carter said of the federal funding. If implemented, the Prairie Shield project would allow first responders in this region −− including police, fire agencies, and others −− to communicate on an "alternate wireless network" during significant emergencies.
Source: http://www.journalstandard.com/articles/2006/01/26/local_new s/news03.txt

31. *January 26, Trentonian (NJ)* — **New Jersey city practices response to large−scale CBRNE incident.** Attendees fall ill minutes after a hockey game concludes. This was the scenario authorities were given during a joint multi−agency hazardous materials response exercise at the Sovereign Bank Arena in Trenton, NJ, Wednesday, January 25. The New Jersey National Guard's 21st Weapons of Mass Destruction−Civil Support Team along with the New Jersey State Police Hazardous Materials Response Unit, Mercer County Office of Emergency Management and the city fire department, participated in the training drill. The exercise tested the teams' skills for the possibility of a large−scale chemical, biological, radiological, nuclear and explosive (CBRNE) incident, said Lt. William McDonald, head of the hazardous materials response unit with the state police. McDonald said the scenario for the exercise −− which began around 8 a.m. EST and continued throughout the day −− was that an unknown chemical was released inside the arena, following a hockey game. Attendees became sick and unconscious, and teams had to enter for search and rescue drill. Various monitors, taking constant air samples while sending information to a centralized laptop, were placed inside and around the area. The teams wore chemical protective clothing and tested how each other's equipment, such as different communication radio systems, worked together.
Source: http://www.zwire.com/site/news.cfm?newsid=16005186&BRD=1697&PAG=461&dept_id=44551&rfi=6

32. *January 26, Federal Computer Week* — **Department of Homeland Security seeks location−tracking technology.** Department of Homeland Security officials are currently evaluating white papers on technology that could help locate, for example, firefighters and other emergency responders in high−rise buildings. The Homeland Security Advanced Research Projects Agency (HSARPA) issued a broad agency announcement (BAA) last November that sought 22 different prototype technologies, including tracking capability, for emergency responders for various uses. In that HSARPA solicitation −− called the Rapid Technology Application Program −− an Advanced 3−D Locator System would help accurately track and pinpoint first responders in threatened or collapsed buildings or in underground facilities. "Accurate location and tracking is necessary in order to allow emergency managers, including fire chiefs and other incident commanders, to rapidly and effectively deploy and re−deploy their forces or understand and respond to the consequences of potential threats to their forces," according to the BAA. Capt. Vincent Doherty of the New York City Fire Department's hazardous materials operations said his department has been seeking such

technology before the 2001 terrorist attacks, when 343 firefighters and 23 police officers died responding to the World Trade Center emergency.
Source: http://www.fcw.com/article92117−01−26−06−Web

33. *January 26, Indy Channel (IN)* — **Disaster officials' worst−case scenario: Indianapolis flood.** Frightening and thought−provoking questions were raised at a meeting Wednesday night, January 25, about how Indiana emergency officials would handle a catastrophic flood, should one ever happen in Indianapolis. The questions were raised at a disaster−training workshop, where emergency officials put together what they called a worst−case scenario. The worst−case scenario, as officials saw it, could leave many parts of the city, including downtown Indianapolis, under water. The Geist Reservoir is one of the largest bodies of water in central Indiana. Geist was the focal point of the disaster management drill. Emergency managers considered what they would do if the dam at Geist should ever fail, which officials said is extremely unlikely. Planners admitted the worst−case scenario would probably never happen, but as emergency officials, they must be prepared for the almost unthinkable. Planners admitted that Indianapolis is not ready for a catastrophic event. "A number of organizations and agencies still have a long way to go in emergency planning. We're getting closer, but we still have a good ways to go," Indianapolis police Lt. Brian Clouse said. "These discussions help point that out."
Source: http://www.theindychannel.com/news/6459458/detail.html

34. *January 26, Post−Gazette (PA)* — **Training exercise to test readiness of Pennsylvania county's emergency responders.** "Operation Urban Thunder" will begin in Westmoreland County, PA, in October with a simultaneous countywide weather crisis and a weapon of mass destruction in Greensburg. The county court house and city hall will evacuate, and Westmoreland's 4,000−plus emergency responders will scramble to secure the devastated county seat. It's the latest in Westmoreland County public safety department's full−scale training exercises, "the biggest one yet attempted," according to safety director Rich Matason. Urban Thunder will continue for 24 hours, testing the responses of the county's emergency operations center and public safety department, as well as any of the county's 118 fire departments, 38 emergency medical providers, and 40−plus police departments who choose to take part. The faux crisis will strike on a Friday and force city and county officials to enact their emergency backup plans. The "continuity of government" aspect is especially pertinent in light of post−Katrina government breakdowns seen along the Gulf Coast in 2005, Matason said. But make−believe trauma is only a part of the 2006 plan, Matason said. The county's much−touted 800−megahertz emergency radio system still needs improving, and the department is applying for grants to buy repeater units to better serve weak areas.
Source: http://www.post−gazette.com/pg/06026/644101.stm

[Return to top]

Information Technology and Telecommunications Sector

35. *January 26, FrSIRT* — **Cisco VPN 3000 concentrator remote denial of service vulnerability.** A vulnerability has been identified in Cisco VPN 3000 series concentrators, which could be exploited by remote attackers to cause a denial of service. The error in the HTTP service (enabled by default) that does not properly handle specially crafted requests,

which could be exploited by remote attackers to cause a vulnerable device to reload and drop user connections. Solution: Upgrade to Cisco VPN 3000 series software version 4.7.2.B or later: http://www.cisco.com/pcgi−bin/tablebuild.pl/vpn3000−3des
Source: http://www.frsirt.com/english/advisories/2006/0346

36. *January 26, FrSIRT* — **Sophos anti−virus products ARJ archives security bypass vulnerability.** A vulnerability has been identified in various Sophos anti−virus products, which could be exploited by attackers or malware to bypass scan detection measures. This flaw is due to an error in the anti−virus engine that does not properly handle specially crafted ARJ archives, which could be exploited by attackers or malware to prevent a vulnerable antivirus from scanning infected or malicious archives. Solution: This vulnerability has been fixed in Sophos anti−virus versions 5.1.4, 4.5.9, 4.6.9 and 4.02.
Source: http://www.frsirt.com/english/advisories/2006/0347

37. *January 26, Hackers Center Security Portal* — **Microsoft Internet Explorer does not honor ActiveX.** Internet Explorer (IE) fails to properly check the kill bit for ActiveX controls, which may allow a remote attacker to execute arbitrary code on a vulnerable system. By convincing a user to view a specially crafted HTML document an attacker could execute arbitrary code with the privileges of the user. Depending on the ActiveX control being used, an attacker may be able to take other actions. There are a number of significant vulnerabilities in technologies involving the IE domain/zone security model, local file system (Local Machine Zone) trust, the Dynamic HTML (DHTML) document object model in particular, proprietary DHTML features; the HTML Help system, MIME type determination, the graphical user interface (GUI), and ActiveX. These technologies are implemented in operating system libraries that are used by IE and many other programs to provide Web browser functionality. IE is integrated into Windows to such an extent that vulnerabilities in IE frequently provide an attacker significant access to the operating system.
Source: http://www.hackerscenter.com/archive/view.asp?id=22251

38. *January 26, Security Focus* — **Researchers: Rootkits headed for BIOS.** Insider attacks and industrial espionage could become stealthier by hiding malicious code in the core system functions available in a motherboard's flash memory, researchers said on Wednesday, January 25, at the Black Hat Federal Conference. A collection of functions for power management, known as the Advanced Configuration and Power Interface (ACPI), has its own high−level interpreted language that could be used to code a rootkit and store key attack functions in the Basic Input/Output System (BIOS) in flash memory, according to John Heasman, principal security consultant for UK−based Next−Generation Security Software. The researcher tested basic features, such as elevating privileges and reading physical memory, using malicious procedures that replaced legitimate functions stored in flash memory. "Rootkits are becoming more of a threat in general −− BIOS is just the next step," Heasman said during a presentation at the conference. "While this is not a threat now, it is a warning to people to look out." The worries come as security professionals are increasingly worried about rootkits. While some attacks have attempted to affect a computer's flash memory, the ability to use the high−level programming language available for creating ACPI functions has opened up the attack to far more programmers.
Source: http://www.securityfocus.com/news/11372

39. *January 26, eWeek* — **Oracle advises users: Patch critical hole −− now.** Oracle is advising its customers to quickly apply a database patch for a flaw security experts are calling "very severe." Security experts warn the hole could allow even unsophisticated users to take control of Oracle databases. The patch, known as DB18, fixes a hole that affects most supported versions of the Oracle database software, including Oracle versions 8, 9 and 10. The hole is "very severe" and allows users to bypass the Oracle database's authentication and become administrative "super users," according to Shlomo Kramer, CEO of Imperva, which discovered the hole. However, Kramer and others say Oracle may be downplaying the seriousness of the threat out of concern that malicious hackers could be tipped off to the severity of the issue. Oracle Corp. said that it patches security holes in the order of their severity and categorized DB18 as a serious vulnerability with the potential for wide impact in the January Critical Patch Update [CPU], according to an e−mail statement. Researchers in Imperva's Application Defense Center discovered the security hole "a few months ago," though it has existed for years, Kramer said. "It goes all the way back to Version 8, but it wasn't patched until now."
Source: http://www.eweek.com/article2/0,1895,1915359,00.asp

40. *January 26, CNET News* — **Politicians call for better phone record privacy.** In response to disclosures about phone records being sold on the Internet, politicians want federal regulators to verify that the biggest service providers are adequately protecting their customers' information. According to a letter sent by the chairmen of the U.S. House of Representatives Energy and Commerce Committee, all telecommunications providers must "certify annually" with the Federal Communications Commission (FCC) that they are in compliance with the federal rules. The politicians asked the FCC to turn over the latest certifications from the five largest wireless and wireline providers, along with statements from the companies describing "how their internal procedures protect the confidentiality of consumer information." Citing their ongoing investigation about the matter, the legislators imposed a Monday, January 30, deadline. The House returns from its winter recess Tuesday, January 31. The issue of the illicit brokering of phone records has drawn attention recently, with carriers such as T−Mobile, Verizon Wireless and Cingular Wireless and also the state of Illinois filing suits against third−party brokers accused of the practice. On Monday, January 23, T−Mobile landed a temporary restraining order, which prohibits at least two companies from directly or indirectly obtaining its customers' information.
Letter sent by the chairman of the U.S. House of Representatives Energy and Commerce Committee: http://markey.house.gov/docs/privacy/iss_privacy_ltr060123.p df
Source: http://news.com.com/Politicians+call+for+better+phone+record+privacy/2100−1036_3−6031916.html?tag=cd.top

41. *January 26, eWeek* — **Apple's switch to Intel could allow OS X exploits.** The recent move by Apple Computer to begin shipping Macintosh computers that use microprocessors from Intel could open the door to more attacks against computers running the company's OS X operating system, security experts warn. The change could put more pressure on Apple to build security features into OS X. In an e−mail statement, the company said that the security technologies and processes that have made Mac OS X secure for PowerPC remain the same for Intel−based Macs. However, using the Intel x86 platform pulls Macintosh systems onto the same platform used by Microsoft's Windows computers, a prime target of the hacking community for years. "Attackers have been focused on the [Intel] x86 for over a decade. Macintosh will have a lot more exposure than when it was on PowerPC," said Oliver Friedrichs, a senior manager at

Symantec Corp. Security Response. There are many more malicious hackers who understand the x86 architecture in−depth than understand the PowerPC. And attackers have access to hundreds of documents and examples of how to exploit common vulnerabilities on x86, whereas exploits for PowerPC are far fewer, Friedrichs said.
Source: http://www.eweek.com/article2/0,1895,1915923,00.asp

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 receiving reports of a new destructive email worm known as CME 24, which will actively disable anti−virus software on a host system and will also overwrite users' data files on the third of every month. This worm affects all recent versions of Microsoft Windows. CME 24 is also known as Nyxem.E, Blackmal.E, MyWife.d, BlackWorm, Tearec.A, Grew.a, and Kama Sutra.

This malcode spreads primarily by harvesting email addresses from files on the local machine and then emailing itself as an executable attachment. It uses subject lines such as "Photos", "*Hot Movie*", and "Miss Lebanon 2006" to entice the user into opening the attachment. As soon as the attachment is executed, the user's system is immediately infected. Infected hosts within a network enclave will also try to spread locally through network shares with weak passwords.

On the third of every month, CME 24 will over−write users' files on all accessible drives with the message "DATA Error [47 0f 94 93 F4 F5]". This will happen approximately 30 minutes after the user logins to the infected machine. The files affected by this variant will have the following file extensions: .doc, .xls, .mdb, .md3, .ppt, .pps, .zip, .rar, .pdf, .psd, and .dmp.

The infected host will also access a website containing a counter. The web counter shows how many machines have been infected, although it is expected that an infected machine may access that website on multiple occasions, thus inflating the number. The web counter has shown consistent growth with over 500,000 infections on Saturday and is now currently showing over 700,000 infections. FBI agents have received log data that resided on the web server, and is sharing the bulk data with US−CERT for analysis.

As CME 24 disables anti−virus systems, it leaves infected computers wide open to attack by other malware variants. All major anti−virus companies are offering signature files that should prevent infection. In addition, major anti−virus vendors are offering tools and instructions for removing this variant from their systems.

US−CERT has not received any reports of infections within the Federal space. Currently, US−CERT is coordinating the analysis of log file data that could be an indicator of infected systems, and will be distributing notifications to affected parties.

Nyxem Mass−mailing Worm US−CERT is aware of a new mass mailing worm known as Nyxem (CME−24). This worm relies on social engineering to propagate. Specifically, the user must click on a link or open an attached file.The Nyxem worm targets Windows systems that hide file extensions for known file types (this is the default setting for Windows XP and possibly other versions). The worm's icon makes it appear to be a WinZip file. As a result, the user may unknowingly execute the worm. For more information please review: http://cme.mitre.org/data/list.html#24

US−CERT strongly encourages users not to follow unknown links, even if sent by a known and trusted source. Users may also wish to visit the US−CERT Computer Virus Resources for general virus protection information at URL: http://www.us−cert.gov/other_sources/viruses.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 6346 (gnutella−svc), 445 (microsoft−ds), 4556 (−−−), 25 (smtp), 6348 (−−−), 139 (netbios−ssn), 32768 (HackersParadise), 54000 (−−−) 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

42. *January 27, Associated Press* — **NORAD rehearsing Super Bowl security.** The North American Aerospace Defense Command (NORAD) on Thursday, January 26, practiced its plan to protect Detroit's Ford Field from an air attack on Super Bowl Sunday, February 5, a concern spawned by the terrorist attacks of September 11, 2001. The exercise run by the joint Canadian and American command, which defends North American from missile and air attacks, was hampered by "weather issues" and will be redone next week, Canadian Forces Maj. Darren Steele said. Hundreds of people, including controllers, fighter pilots, an E−3 Airborne Early Warning and Control System aircraft, several civilian aircraft, and air refueling tankers took part in the exercise. Next Wednesday, February 1's exercise will be on the same scale. Since the September 11 attacks, NORAD jets have patrolled the skies through Operation Noble Eagle. Fighters have responded to more than 2,000 air events in the United States and Canada and have flown more than 40,000 sorties.
Source: http://www.king5.com/sports/stories/NW_012706SHBnoradJG.43e2 db62.html

43. *January 27, Reuters* — **Italy on alert for terror at winter games.** Italy is prepared for any kind of terrorist attack linked to the Winter Olympics and is ready to re−introduce border controls if necessary ahead of the games that begin in two weeks, top security officials said on

Friday, January 27. The security and Interior Ministry officials briefing reporters also said that security agents coming in with teams for the February 10−26 games in the Turin area of northern Italy would not be allowed to carry their own weapons. They said Italy was ready for any eventuality that might disrupt the games and had set up a special squad to react to nuclear, biological, chemical or dirty−bomb threats. "At this time we are not aware of any terrorist threat," one top security official said. "But experience teaches us that the overlapping of several big, important events, such as the elections (and the Olympics) can be a temptation, a time of danger, and this is why our level of attention is at a very high level," he said. The campaign for Italy's national elections in April will start officially on February 11, one day after the games start.
Source: http://ca.today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006−01−27T163134Z_01_L27274942_RTRIDST_0_NEWS−OLYMPICS−SECURITY−COL.XML&archived=False

[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

material.