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

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

Daily Highlights

- The Associated Press reports utility crews were working nonstop through the weekend to restore service to hundreds of thousands of people still without power after a windstorm hit western Washington state on Thursday, December 14; it could be several days before everyone has power again. (See item 1)
- The Department of Homeland Security issued on Friday, December 15, a notice of proposed rulemaking, as part of a package of new security measures to vastly strengthen the security of the nation's rail systems in the highest threat urban areas. (See item 14)
- The Glendale, Arizona, police bomb squad was called out early Wednesday, December 13, after a number of homemade explosive devices were found inside a storage locker. (See item 43)

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. *December 16, Associated Press* — **Utility crews work to restore power to wind−swept Washington.** Utility crews were working nonstop through the weekend to restore service to hundreds of thousands of people still without power after a windstorm hit western Washington

state. The storm hit late Thursday, December 14. At its peak, the storm knocked out power to more than a million people in western Washington. Puget Sound Energy had restored power to about 260,000 customers by Saturday afternoon, leaving 440,000 still without. It could be several days before everyone is restored. The utility suffered extensive damage to its transmission system. About 250 repair crews were on the job Saturday and another 100 were being called in over the next two days, company spokesperson Dorothy Bracken said. By midday Saturday, more than 57,100 people remained without power in Seattle, down from Seattle City Light's peak of 175,000. Another 15,000 were still without power in the Snohomish County Public Utility District north of Seattle, down from 120,000 earlier. Tacoma Public Utilities had about 11,000 customers still without power, down from roughly 100,000 on Friday. Between 5,000 and 6,000 customers remained without power in Grays Harbor County on the coast, with scattered outages throughout Ocean Shores and around Lake Quinault.
Source: http://www.kgw.com/sharedcontent/APStories/stories/D8M26M800 .html

2. *December 15, U.S. Department of Energy* — **U.S. and China announce cooperation on FutureGen and sign Energy Efficiency protocol at U.S.−China Strategic Economic Dialogue.** The U.S. and China Friday, December 15, announced that China will join the Government Steering Committee of the FutureGen project making China the third country to join the U.S. in the FutureGen International Partnership. The U.S. and China also signed an Energy Efficiency and Renewable Energy Protocol renewing cooperation in advancing clean technology including solar, wind, and biomass. The agreements were made as an outcome of the U.S.−China Strategic Economic Dialogue (SED) in Beijing. The $1 billion FutureGen initiative is a ten−year effort announced by President Bush in 2003. FutureGen will initiate operations in 2012 and will be the first plant in the world to produce both electricity and commercial−grade hydrogen from coal, simultaneously. The U.S.−China Energy Efficiency and Renewable Energy Protocol renews the joint collaboration in developing and deploying clean, energy efficient and renewable energy technology including solar, wind, biomass, geothermal, and hydrogen energy. Other cooperative efforts between the U.S. and China include the Asia Pacific Partnership on Clean Development and Climate; the International Partnership for a Hydrogen Economy; the Carbon Sequestration Leadership Forum; the International Thermonuclear Experimental Reactor; and the Generation IV International Forum.
Source: http://www.energy.gov/news/4535.htm

3. *December 15, Sun−Sentinel (FL)* — **Transformer explodes at FPL power plant at Port Everglades.** The Broward, FL Sheriff's Office and firefighters responded to an explosion and fire Thursday night, December 14, at a Florida Power & Light generating plant inside Port Everglades. The 8:40 p.m. EST blaze took out 12 gas turbine units, used for back up during peak electricity usage in Broward County, said FPL spokesperson Karen Vissepo. There were no resulting power outages. Broward Sheriff's Office spokesperson Jim Leljedal said a deputy on patrol saw a transformer explode inside the Florida Power & Light (FP&L) compound and called in firefighters, who fought the transformer blaze and burning brush. That fire was under control 40 minutes later. Not knowing the cause of the explosion, deputies closed off the port in case of a security breach. The port was reopened about an hour later. The shutdown inconvenienced several gasoline tanker drivers but had no major impact. Deputies reported that lights flickered in the area immediately after the mishap.
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−1215 portexplosion,0,5950486.story?coll=sfla−home−headlines

4. *December 11, Government Computer News* — **DHS, industry use LOGIIC to combat cyberthreats at oil and gas facilities.** The Department of Homeland Security (DHS) has teamed with 13 organizations on a 12−month project to secure the process control systems of the nation's oil and gas industries against cybersecurity threats. A cyberattack on the control and data systems of electric power plants, or oil and gas refineries and pipelines −− two of 17 pieces of the nation's critical infrastructure −− could potentially bring the country to a halt. The problem is compounded because private companies control 85 percent to 90 percent of the country's critical infrastructure −− leaving the government few avenues to ensure that IT systems are secure. Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) was born out of the Cyber Security Research and Development Center, which is supported by DHS. LOGIIC brought government, industry, research labs, security vendors and process control technology vendors together to recreate a real−life process control system test bed. They then attacked the test bed, at Sandia National Laboratories in Albuquerque, NM, with viruses, worms and cyberterrorism techniques to see if they could fix system vulnerabilities.
Source: http://www.gcn.com/print/25_34/42765−1.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *December 15, IDG News Service* — **Former Chinese national faces charges of stealing military application trade secrets and selling them to foreign governments.** A former Chinese national is facing U.S. federal charges of stealing trade secrets from a Silicon Valley company and selling them to foreign governments. The U.S. Attorney's Office in San Francisco Thursday, December 14, filed a 36−count indictment in U.S. District Court for Northern California against Xiaodong Sheldon Meng accusing him of stealing military application trade secrets from Quantum3D, of San Jose, CA, and using them to try to sell the technology to the People's Republic of China, the Malaysian Air Force, and the Thailand Air Force. Quantum3D designs high−end graphics computers that run visual simulation training software for military applications such as flight simulators. Meng, a one−time employee of Quantum3D, stole the trade secrets with the intent that they would be used to benefit those foreign governments, according to the U.S. Attorney Kevin V. Ryan.
Source: http://www.infoworld.com/article/06/12/15/HNtradesecretsthef t_1.html

[Return to top]

Banking and Finance Sector

6. *December 15, USA TODAY* — **Banks and credit card agencies are gearing up security for financial transactions over cell phones and other handheld devices.** Aware that a growing

number of consumers −− especially those under 35 −− are comfortable using cell phones as digital wallets, leading financial institutions are concocting mobile−security options to protect them from hackers and cyberthieves. "Mobile banking is where online banking was a decade ago. It's starting to take off," says Richard Crone, a Silicon Valley consultant who follows electronic−payment services. Wachovia's 5.9 million customers now have the option of using a cell phone or personal digital assistant to check accounts and transfer funds. The mobile service requires an encrypted user name and password. To check balances, pay bills, transfer funds and search for a nearby ATM from cell phones, Citi Mobile requires an access code and operates on an encrypted system. Under a system being tested by Visa USA, mobile−device users need to enter a password to perform financial tasks. MasterCard Worldwide is offering mobile authentication, which lets consumers shop or bank but they are required to enter a PIN. Financial institutions are building digital defenses as mobile viruses rise. Mobile viruses have increased from 34 in 2004 to 162 in 2006, says security firm SMobile Systems. SMobile expects 600 to 700 new viruses in 2007.
Source: http://news.yahoo.com/s/usatoday/20061215/tc_usatoday/ascell phoneusesgrowsodosecurityoptions

7. *December 15, VNUNet* — **Victims of identity theft top 100 million.** More than 100 million U.S. individuals have had personal information stolen since early 2005, according to an overview published by the Privacy Rights Clearinghouse (PRC). The counter passed the 100 million mark on Wednesday, December 13, when Boeing admitted that it had lost a laptop containing confidential information including social security numbers for 382,000 current and former employees. The PRC maintains a Website that tracks cases of identity theft and accidental data disclosures. But the 100 million figure is just the "tip of the iceberg," warned PRC director Beth Givens. The number of breached data records in many cases is unknown.
PRC Website: http://privacyrights.org/
Source: http://www.vnunet.com/vnunet/news/2171073/identity−theft−vic tims−surpass

8. *December 14, Christian Science Monitor* — **Real estate fraud rises in U.S.** Real estate fraud has now firmly emerged on the FBI's radar as the country's fastest−growing white collar crime. Industry losses ran to at least $606 million last year, it says. And the Treasury Department's suspicious−activity reports are up 35 percent this year. The Internal Revenue Service's criminal case numbers in mortgage fraud have been doubling every two years through the first half of this decade. If the real estate downturn continues past 2007, experts say the implications for the economy could be dire. Georgia is a major hot spot of mortgage fraud, where metro Atlanta has become known as the mortgage fraud capital of the U.S., according to rankings by Fannie Mae. New automated lending procedures, aimed at eliminating discrimination, has made it easier for fraudulent applications to slip through. The decline of local banking in favor of nationalized mortgage syndicates also contributes to fraud, as does the recent move toward sub−prime, high−interest loans. Opportunity for both large and small scams by a coterie of real estate professionals, combined with secretive and decentralized lending structures, means the system is ripe for abuse, experts say. Critics say what's needed is a national lenders' clearinghouse and more federal regulation.
Source: http://www.csmonitor.com/2006/1214/p02s01−usec.html

9. *December 14, Greenwood Commonwealth (MS)* — **Teenagers possible source of counterfeit currency circulating in Itta Bena, Mississippi.** Itta Bena, MS, Police Chief Coy Lee Keys

says merchants in his town are suffering from an epidemic of funny money. "I've got $1,000 in counterfeit bills. They've been passed over a month's period of time. This is the season when this happens," the chief said. The U.S. Secret Service, which enforces federal counterfeiting laws, has been contacted regarding the phony $100 and $20 bills circulating in the town, but Keys said a federal investigation isn't likely to happen soon. Keys said a major outbreak of phony bills occurred recently at Leflore County High School. The chief believes youngsters are being used to circulate the fake bills in the community. “The adults figure if they do it they could face some serious jail time, so they get the kids to do it,” he said. Keys is concerned that merchants, experiencing a rush of customers during the holiday season, might not examine the bills before accepting them.
Source: http://www.zwire.com/site/news.cfm?newsid=17591506&BRD=1838&PAG=461&dept_id=104621&rfi=6

10. *December 14, Associated Press* — **Authorities arrest New York City counterfeit goods ring trying to flood holiday market.** Department of Homeland Security agents seized more than $6 million worth of foreign−made fake clothing and shoes smuggled into the United States and sold under famous labels including Nike, Sean Jean and Lacoste, authorities reported on Thursday, December 14. Four people were arrested as members of a counterfeit ring that stretched from New Jersey and New York to Texas, according to a federal complaint filed by U.S. Attorney Michael J. Garcia. The apparel industry "is increasingly threatened by counterfeiters who sell fake trademarked goods to sometimes unwitting customers," Garcia said in a statement. The case was a joint effort between federal prosecutors and Homeland Security's Immigration and Customs Enforcement (ICE) unit. Martin D. Ficke, a special agent with ICE, said he expected millions of dollars more in counterfeit goods to surface. According to the criminal complaint, the merchandise was produced in countries including Pakistan and China and smuggled into the United States through two New Jersey ports and John F. Kennedy International Airport. As a result of the ongoing probe, authorities have conducted 66 seizures. Agents executed search warrants at warehouses and offices in New Jersey, Manhattan, NY, and Houston, TX.
Source: http://www.iht.com/articles/ap/2006/12/15/business/NA_FIN_US_Knockoff_Bust.php

[Return to top]

Transportation and Border Security Sector

11. *December 17, Gannett News Service* — **Union: Fewer air controllers could lead to more mistakes.** Nearly 1,100 fewer air traffic controllers are guiding planes through the nation's skies than three years ago, even though flights are increasing. The National Air Traffic Controllers Association, the union that represents those who "move tin," says some facilities are critically understaffed, causing delays and increasing the possibility of mistakes by tired controllers working 10−hour days and six−day weeks. The union claims staffing problems played a role in three air crashes this year, including the August 27 crash of a Comair jet in Lexington, KY, that killed 49 of 50 people aboard. Staffing numbers provided to Gannett News Service by the union show that towers or radar facilities in northern California, Dallas, Detroit, New York, Washington−Dulles, and other high−volume locations are moving airplanes with as few as 69 percent to 76 percent of the number of controllers that the Federal Aviation Administration and the union agreed constituted full staffing in 2003, the most recent

benchmark. Internal FAA operations logs reveal that staffing problems have caused controllers to increase the separation, or distance, between planes out of Charlotte, NC, Washington−Dulles, and New England airports in November.
Source: http://www.usatoday.com/travel/flights/2006−12−17−air−traffi c_x.htm

12. *December 16, Associated Press* — **Fire on plane forces landing in Colorado.** A personal air filter sparked a fire Friday, December 15, on Continental Airlines Flight 1065 −− with 154 passengers and six crewmembers aboard flying from Houston to Portland, OR −− forcing an emergency landing. Six people were taken to a hospital, officials said. Flight attendants put out the flames, and the plane landed safely at around 5 p.m. MST, Continental spokesperson Julie King said. The battery−powered device, which is worn around the neck and filters air near the person wearing it, malfunctioned and sparked a fire, King said.
Source: http://www.usatoday.com/news/nation/2006−12−16−plane−fire_x. htm

13. *December 15, USA TODAY* — **Travel industry sets up 'one−stop' passport shop.** Eager to see an unimpeded flow of travelers into the USA once new passport regulations take effect next month, the Travel Industry Association this week launched a Website to provide "one−stop shopping" for passport applicants. Beginning January 23, all air travelers, including Americans, entering the U.S. from Canada, Mexico, and the Caribbean (excluding Puerto Rico and Virgin Islands) must show a passport. The new Website has links to appropriate agencies for U.S., Canadian and Mexican citizens, although they still will need to apply for new passports in person.
Website: http://getapassportnow.com/
Source: http://www.usatoday.com/travel/news/2006−12−14−passport_x.ht m

14. *December 15, Department of Homeland Security* — **DHS targets high risk hazardous materials in transit.** The Department of Homeland Security (DHS) issued on Friday, December 15, a notice of proposed rulemaking to vastly strengthen the security of the nation's rail systems in the highest threat urban areas. The proposed rule is part of a package of new security measures that will require freight rail carriers to ensure 100 percent positive hand−off of Toxic Inhalation Hazard (TIH) materials, establish security protocols for custody transfers of TIH rail cars in the high threat urban areas, and appoint a rail security coordinator to share information with the federal government, as well as formalizing the Transportation Security Administration's (TSA) freight and passenger rail inspection authority. The freight rail industry has already begun to implement several key security measures, such as tracking and substantially reducing the standstill time for unattended freight cars transporting TIH materials in high threat urban areas, developing site−specific security plans with access controls, and providing security training for employees. TSA has the authority to impose up to $10,000 in fines per security violation, per day. The rule will be posted to the Federal Register on December 21, and it will be open for public comment for 60 days.
TSA's proposed rule is available at http://www.tsa.gov/
Source: http://www.dhs.gov/xnews/releases/pr_1166200220343.shtm

15. *December 15, Department of Homeland Security* — **DHS announces $12 million for Operation Stonegarden.** The Department of Homeland Security (DHS) announced on Friday, December 15, more than $12 million in grant awards to the four Southwest border states in support of ongoing local law enforcement efforts at the border. The funding, as part of

Operation Stonegarden, assists local authorities with operational costs and equipment purchases that contribute to border security. The distribution of these funds is as follows: Arizona, $6,353,174; California, $1,000,000; New Mexico, $1,580,258; and Texas, $3,070,081. Operation Stonegarden began as a successful pilot program in fiscal year 2005 that involved 14 border states. The initiative gave states the flexibility to use DHS grant funding to enhance coordination among state and federal law enforcement agencies at our borders. The pilot program resulted in an estimated 214 state, local and tribal agencies working 36,755 man−days on various public safety and border security operations. Funding for Operation Stonegarden was made available through the fiscal year 2006 Emergency Supplemental Appropriations Act for Defense, the Global War on Terror and Hurricane Recovery. The program requires states to identify and prioritize solutions to their border security needs.
Source: http://www.dhs.gov/xnews/releases/pr_1166216119621.shtm

16. *December 15, Department of Transportation* — **Department of Transportation proposes to require railroads to route hazardous materials based on range of safety and security factors.** Railroad companies would be required to perform a safety and security risk analysis to determine the most appropriate route for shipping hazardous materials as part of a new proposal announced Friday, December 15, by Department of Transportation (DOT) Secretary Mary Peters. The Secretary said the notice of proposed rulemaking, issued by the Department of Transportation's Federal Railroad Administration and Pipeline and Hazardous Materials Safety Administration, would make shipments of certain high−risk hazardous materials, including explosives, radioactive substances and toxic−inhalation risk materials, more safe and secure by adding to and strengthening existing federal regulations. Under the proposed rule, rail carriers would be required to compile annual data clearly identifying route segments and the total number and type of hazardous materials shipments transported over each route and use the information to analyze the safety and security risks present on each route. Railroads would then be required to use this data to select the route that provides the highest possible degree of safety and security. The Department's proposal was developed in coordination with the Department of Homeland Security's Transportation Security Administration, which also issued proposed rules designed to address a range of rail hazardous materials transport security issues.
A copy of notice is available at http://www.phmsa.dot.gov/.
Source: http://www.dot.gov/affairs/dot11606.htm

17. *December 15, Associated Press* — **Power outage affects Sea−Tac flights.** Many flights at Seattle−Tacoma International Airport (Sea−Tac) were canceled or delayed Friday, December 15, stemming from a power outage apparently caused by a strong windstorm that blew through the region. A Federal Aviation Administration (FAA) office that tracks planes was shut down from about 4:30 p.m. to 5:30 p.m. PST so its operations could be transferred to another control center in nearby Auburn, airport spokesperson Rachel Garson said. That Terminal Radar Approach Control building is where air−traffic controllers communicate with all flights within 25 miles of the airport. Once flights are within a five−mile radius, communication is transferred to the air−traffic control tower. But the problems began much earlier. Separately from the FAA outage, the airport's south end lost power at about 1:30 a.m. Friday, and many flights were canceled or delayed beginning about that time, affecting "thousands" of passengers, Garson said. The outage affected ticketing counters, several baggage−claim carousels, the baggage handling area and the A gates, where American and Delta airlines flights arrive and depart. Because of the outage, a nationwide "ground stop" was issued for flights bound for Sea−Tac.

Source: http://www.columbian.com/news/APStories/AP12162006news84822. cfm

18. *December 13, KTVU (CA)* — **Search for laser pointed at commercial jets.** A raid staged at a San Jose, CA, home was the latest attempt by Santa Clara and federal authorities to find the source of a blinding laser beam that is being flashed into the cockpits of commercial aircrafts trying to land in the Bay Area. Serge Palanov, a spokesperson from the Santa Clara Sheriff's Department, said deputies searched a home near Cambrian Village −− about seven miles south of San Jose's Mineta International Airport −− on Monday, December 11. "We received several calls from the Federal Aviation Administration and from citizens stating that there was a green laser emanating from a residence pointing at some commercial airliners," Palanov said. "Our own helicopter −− Star One −− went up in the air into vicinity and they also experienced this green laser pointing at them." Lasers −− small lasers commercially available and used commonly as light pointers −− can beam a high intensity light over a long distances. If the beam were to strike a pilot's eyes, it could blind him or her. San Francisco International Airport spokesperson Mike McCarron −− a former Navy airman −− said lasers, even small seemingly harmless ones, can be threatening to the safety of the airplane and its passengers.
Source: http://www.ktvu.com/news/10524793/detail.html

19. *December 12, Jersey Journal (NJ)* — **Suspicious fire destroys train cargo.** A fire Monday morning, December 11, on board a freight train carrying dozens of new cars has been labeled "suspicious" by the Jersey City Fire Department. Authorities were notified at 7:11 a.m. EST by a 911 call reporting a boxcar fire, officials said yesterday. The train, which originated in Georgetown, KY, and is operated by the CSX Corporation, was spotted on fire near Linden and Princeton avenues, said Andrew Johnson, a spokesperson for the Fire Department. Johnson said eight to 12 cars caught on fire and four started to melt. The Fire Department's arson unit was investigating.
Source: http://www.nj.com/news/jjournal/index.ssf?/base/news−3/11659 06975280620.xml&coll=3

[Return to top]

Postal and Shipping Sector

20. *December 16, Associated Press* — **Powder found at United Nations apparently flour.** A suspicious package leaking white powder was found near CNN's office at United Nations (UN) headquarters Friday, December 15, prompting officials to cordon off the area. Preliminary tests showed the substance appeared to be flour, UN officials said. "On the basis of preliminary results, the substance does not appear to be harmful but some tests continue," UN associate spokesperson Farhan Haq said Friday night. "It appears to flour." Nonetheless, more than two−dozen UN staff members and journalists were decontaminated by New York City police experts as a precaution. Those affected had to wash their hands, face, hair, and other exposed areas, seal their clothes in a bag and wear a special decontaminated suit to go home. UN security guards informed the New York City Police Department and the Department of Environmental Protection, who dispatched teams to examine and test the package along with UN security experts, Hag said. Hazardous material experts in yellow suits could be seen along the corridor with large orange plastic bags.
Source: http://hosted.ap.org/dynamic/stories/U/UN_SUSPICIOUS_PACKAGE

?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

[Return to top]

Agriculture Sector

21. *December 15, USAgNet* — **Pennsylvania becomes first state to preserve 3,000 farms.** Pennsylvania is the first state to preserve more than 3,000 farms through its very successful farmland preservation program, Governor Edward G. Rendell said Friday, December 15. The Pennsylvania Farmland Preservation Board Friday preserved 6,854 acres on 69 farms. "Pennsylvania is setting a national standard for farmland preservation, allowing us to keep production agriculture growing in the commonwealth," said Rendell. "In addition to safeguarding the land, we are also preserving the proud tradition of farming, our state's number one industry and one which contributes $45 billion to the economy."
Source: http://www.usagnet.com/story−national.php?Id=2628&yr=2006

22. *December 15, Animal and Plant Health Inspection Service* — **USDA celebrates the opening of a new invasive species research building.** The U.S. Department of Agriculture (USDA) recently celebrated the opening of its new 25,000−square−foot Invasive Species Research Building (ISRB). The building, part of USDA's Animal and Plant Health Inspection Service's wildlife services National Wildlife Research Center (NWRC) headquarters site, is located on 43−acres of the Colorado State University Foothills Research Campus in Fort Collins, CO. "The completion of the Invasive Species Research Building here at NWRC is key to developing innovative methods for resolving new and emerging invasive wildlife species conflicts with agriculture, natural resources, native wildlife and human health and safety," said Bruce Knight, undersecretary for USDA's marketing and regulatory programs mission area. The ISRB enhances NWRC's ability to study the ecology, biology, behavior and physiology of invasive wildlife species and to develop management tools and strategies for mitigating their damage and controlling their spread. The building is designed to simulate temperature and humidity ranges from temperate to tropical ecosystems. The flexibility of these environmental controls allows for the year−round study of invasive wildlife species.
Source: http://www.aphis.usda.gov/newsroom/content/2006/12/isrbcelb. shtml

23. *December 15, Dow Jones* — **FDA, Illinois renew pact to combat mad−cow disease.** The U.S. Food and Drug Administration (FDA) has renewed a cooperative agreement with Illinois to provide federal funds for continued on−farm inspections for bovine spongiform encephalopathy, also known as mad−cow disease, the state of Illinois said Friday, December 15, in a press release. The agreement provides $233,528 for the Illinois Department of Agriculture to inspect 150 farms and analyze 500 feed samples for traces of contaminated cattle feed, the release said. The FDA has prohibited the use of ruminant protein in feed for cattle and other ruminant animals since 1997 because tissue from the nervous system of infected ruminants is believed to spread mad−cow disease. During the two−year agreement, the Illinois Department of Agriculture will also inspect 50 agribusinesses that either sell, blend, or transport cattle feed to make sure no prohibited ingredients are present in their products, said the statement.
Source: http://www.cattlenetwork.com/content.asp?contentid=91608

24. *December 15, Associated Press* — **Fungal infection may have killed ducks.** A fungal infection likely killed 2,500 mallard ducks in a mysterious cluster along a tiny southeastern Idaho creek, a federal wildlife biologist said Friday, December 15. The chances are "extremely high" that Aspergillosis, which can create a fungal toxin on moldy grains and rotting corn, caused the mass die−off, Paul Slota, a biologist with the U.S. Geological Survey's National Wildlife Health Center in Madison, WI, said. Aspergillosis will not spread from bird to bird. All the dead mallards probably ate from the same tainted food source, Slota said. The Wildlife Health Center has already screened nine intestinal tissue swabs from the dead ducks. Each sample showed fungal plaque in the lungs typical of Aspergillosis and tested negative for avian influenza, Slota said.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/12/15/AR2006121501427.html

25. *December 13, Salt Lake Tribune (UT)* — **Whirling disease found in Utah lake.** Anglers are attracted to the Wasatch Plateau in central Utah because there are so many waters. If fishing is slow at one spot they hit the road for a few minutes and try another. That's great for anglers, but state wildlife officials fear that accessibility will help whirling disease spread rapidly across fisheries on the Manti−La Sal National Forest. Division of Wildlife Resources officials announced Wednesday, December 13, that the trout malady that deforms and sometimes kills young trout was confirmed in Electric Lake. There is no evidence of human health issues in eating trout infected with whirling disease.
Source: http://www.sltrib.com/outdoors/ci_4833542

[Return to top]

Food Sector

26. *December 15, Animal and Plant Health Inspection Service* — **USDA expands list of fruits and vegetables eligible for importation.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service announced Friday, December 15, that it has expanded the list of fruits and vegetables eligible, under certain conditions, for importation into the United States. Some of these commodities were previously enterable under a permit but were not listed in the Code of Federal Regulations until now. This action will improve the transparency of our regulations while continuing to protect against the introduction of quarantine pests through imported fruits and vegetables. Each of these additional fruits and vegetables, as a condition of entry, will be inspected and subject to disinfection at the port of first arrival. In addition, some of the fruits and vegetables will be required to be treated or meet other special conditions.
Source: http://www.aphis.usda.gov/newsroom/content/2006/12/fruveglst .shtml

27. *December 15, Dow Jones* — **China pledges to help U.S. meat exporters.** China agreed this week not to punish U.S. exporters immediately for violations discovered in meat and poultry shipments, but rather wait and allow the U.S. to investigate the problem, the U.S. Department of Agriculture Undersecretary for Food Safety said Thursday, December 14. Richard Raymond, a day after his return from meetings in Beijing, said the agreement is aimed at preventing U.S. companies from getting barred from trade. China agreed, Raymond told Dow Jones Newswires in an interview, "that if a product is shipped to China that has some problem with it, they will notify us and give us 45 days to do an evaluation of why we had the problem, work with the

(U.S.) plant (and) reassure China it won't happen again."
Source: http://www.cattlenetwork.com/content.asp?contentid=91300

28. *December 15, Associated Press* — **Taco Bell E. coli outbreak ends; Olive Garden restaurant has illness outbreak.** On Thursday, December 14, Taco Bell Corp. said the Centers for Disease Control and Prevention (CDC) declared an end to the E. coli outbreak linked to lettuce served at its Taco Bell restaurants, and indicated that the lettuce was probably contaminated before reaching the restaurants. The Food and Drug Administration and CDC are still trying to track down the source of the contamination. Now, more than 300 people say they became ill after eating at an Indianapolis−area Olive Garden restaurant last weekend, with patrons reporting symptoms of nausea, vomiting, fever and diarrhea. The nature of the infection hasn't been identified, and area health officials said they found no link to the Taco Bell E. coli outbreak. Olive Garden spokesperson Steve Coe said in an e−mailed statement the outbreak is isolated to one restaurant that will be closed while health officials investigate. He claimed it "may be tied to employees that recently had flu−like symptoms."
Source: http://news.moneycentral.msn.com/provider/providerarticle.aspx?feed=AP&Date=20061215&ID=6281300

29. *December 14, Dow Jones* — **USDA Secretary expects new Japan beef talks in late February.** Japan's unique restriction on U.S. beef −− requiring it come from cattle under 21 months old −− was never meant to be permanent and U.S. Department of Agriculture (USDA) Secretary Mike Johanns said Thursday, December 14, he expects talks to resume in late February to bring about changes that will increase trade. The U.S. and Japan agreed on October 23, 2004, to work toward opening beef trade, but only from the very young cattle. Then, once that occurred and limited amounts of beef were being traded, the two countries agreed to begin a review of applicable international standards on beef safety. Japan began importing U.S. beef again in December 2005, with the under−21−month cattle restriction, but about a month later trade halted again after vertebral column −− prohibited by Japan in U.S. exports −− was discovered in a veal shipment.
Source: http://www.agriculture.com/ag/futuresource/FutureSourceStoryIndex.jhtml?storyId=75800650

[Return to top]

Water Sector

30. *December 14, Water Environment Federation* — **Nation's first physical security standard guidelines for water/wastewater utilities released.** The nation's first standard guidelines for protecting the public from potential malevolent acts and other threats by enhancing the physical security of water and wastewater infrastructure systems were released Thursday, December 14, for trial use by water and wastewater utilities. The guidelines provide drinking water, wastewater and stormwater utilities with practical information to help implement improved security measures in new and existing facilities of all sizes. The documents also address risks from construction and design perspectives and describe physical security approaches for detecting or delaying malevolent parties. The water guideline covers raw water facilities, wells and pumping stations, water treatment plants, water storage facilities, distribution systems and support facilities. The wastewater/stormwater guideline focuses on collections systems, pump

stations, wastewater treatment plants and support facilities.
Draft Guidelines: http://www.wef.org/ScienceTechnologyResources/TechnicalInformation/Projects/security_guidance.htm
Source: http://www.wef.org/NewsCenter/12142006.htm

[Return to top]

Public Health Sector

31. *December 15, Reuters* — **Europe backs Glaxo's pandemic flu vaccine.** A first−generation experimental bird flu vaccine for use in humans from GlaxoSmithKline Plc has won outline support from European regulators. The European Medicines Agency said on Friday, December 15, it had recommended granting a license to Daronrix, a "mock−up" vaccine that could be used as the base for producing a shot to protect people in the event of a pandemic triggered by bird flu. Daronrix is the first vaccine to win such endorsement. But it would only be used once a pandemic has officially been declared and would not be stockpiled in its current form, since it will have to be adapted to include the exact pandemic virus strain. As such it marks just one approach in vaccine preparations. Glaxo, like several of its rivals, is also working on a second−generation vaccine against the H5N1 virus. Its second vaccine is more flexible and could potentially be used as part of a pre−pandemic vaccination campaign.
Source: http://health.yahoo.com/news/170000;_ylt=AmIWHUT0RyGiVMfzho. aBLimxbAB

32. *December 15, Reuters* — **Technology developed to check drug authenticity.** A vendor said on Friday, December 15, it has developed technology to help drug distributors, manufacturers and retailers prevent counterfeit drugs from making their way into the market. The product works using an existing technology: radio frequency identification devices that each have a unique ID transmitted via tiny radio antennas incorporated into a drug's packaging. Computer receivers pick up the data at various transit points in the drug distribution channel, making it easy to track a package's location and also update inventory records.
Source: http://today.reuters.com/news/articleinvesting.aspx?view=CN&storyID=2006−12−15T154308Z_01_N15295031_RTRIDST_0_IBM−PHARMACEUTICALS.XML&rpc=66&type=qcna

33. *December 14, Associated Press* — **Case of mumps confirmed at Eastern Illinois University.** A case of the mumps has been confirmed at Eastern Illinois University, but officials said Thursday, December 14, the chance of an outbreak is unlikely. Illinois has reported at least 600 confirmed cases of the mumps this year, compared with an annual average of about 10 cases in recent years. Federal health experts have called a mumps outbreak that began in Iowa last December and spread to other Midwest states the largest in almost two decades.
Source: http://www.belleville.com/mld/belleville/news/politics/16243 521.htm

34. *December 13, U.S. Department of Health and Human Services* — **United States officially accepts new International Health Regulations.** Department of Health and Human Services Secretary Mike Leavitt on Wednesday, December 13, announced the United States has formally accepted the revised International Health Regulations (IHR), and will begin the process of implementing these new international rules immediately instead of waiting for them to take

effect in June 2007. Secretary Leavitt made the announcement during a week−long visit to the People's Republic of China. The International Health Regulations are an international legal instrument that governs the roles of the World Health Organization and its member countries in identifying and responding to and sharing information about public health emergencies of international concern. The updated rules are designed to prevent and protect against the international spread of diseases, while minimizing interference with world travel and trade. Many of the provisions in the new regulations are based on experiences gained and lessons learned by the global community over the past 30 years.
More information about the IHR is available at: http://www.who.int/csr/ihr/en/
Source: http://www.dhhs.gov/news/press/2006pres/20061213.html

35. *December 13, University of Wisconsin−Madison* — **Scientists find potential weapon against tuberculosis infection.** The discovery of a unique copper−repressing protein in the bacterium that causes tuberculosis in humans may pave the way toward new strategies for halting tuberculosis infection. Scientists have known that when macrophages −− the host's immune cells −− swallow an invading bacterium, they dump excessive amounts of copper onto the invader in an effort to kill it. While all cells need copper to function, too much of the metal ion causes cell death. "But the invaders fight back with their own defense," says Adel Talaat, a microbiologist at the University of Wisconsin−Madison School of Veterinary Medicine. "They block the excess copper." In a paper published in the January 2007 issue of Nature Chemical Biology, Talaat and colleagues from Texas A&M University and University of Saskatchewan in Saskatoon, Canada describe a unique protein repressor that they have identified as the mechanism used by invading bacterium cells to fight off the host's copper attack. Prior to the discovery of this repressor protein, scientists did not know exactly how invading bacterium protected themselves from copper ions used by the body as a defense against infection.
Abstract: http://www.nature.com/nchembio/journal/vaop/ncurrent/abs/nch embio844.html
Source: http://www.news.wisc.edu/13290.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

36. *December 15, VNUNet* — **Vonage users get emergency lifeline.** Vonage America said Friday, December 15, that over 93 percent of its U.S. subscriber lines are now equipped with the Enhanced 911 (E911) emergency calling service. The E911 functionality incorporates a feature that automatically associates a physical address with the calling party's telephone number. Vonage's nomadic E911 implementation allows customers to reach a Public Safety Answering Point, or 911 center, through the dedicated 911 network infrastructure. A customer's call is automatically routed to the appropriate 911 center, with the caller's registered street address and telephone number appearing on the dispatcher screen regardless of where or what exchange they are calling from.

Source: http://www.vnunet.com/vnunet/news/2171102/vonage−users−voip− emergency

37. *December 15, Government Accountability Office* — **GAO−07−169: National Flood Insurance Program: New Processes Aided Hurricane Katrina Claims Handling, but FEMA's Oversight Should Be Improved (Report).** In August and September 2005, Hurricanes Katrina and Rita caused unprecedented destruction to property along the Gulf Coast, resulting in billions of dollars of damage claims to the National Flood Insurance Program (NFIP). This report, which the Government Accountability Office (GAO) initiated under the authority of the Comptroller General, examines (1) the impact of Hurricanes Katrina and Rita on the NFIP and paid losses by location and property type; (2) the challenges the Federal Emergency Management Agency (FEMA) and others faced in addressing the needs of NFIP claimants and communities; (3) FEMA's methods of monitoring and overseeing claims adjustments; and (4) FEMA's efforts to meet the requirements of the Flood Insurance Reform Act of 2004 to establish policyholder coverage notifications, an appeals process for claimants, and education and training requirements for agents. To conduct these assessments, GAO interviewed FEMA and insurance officials, analyzed claims data, and examined a sample of reports done on the accuracy of claims adjustments. GAO recommends that FEMA analyze the overall results of reinspection reports on the accuracy of claims adjustments for future floods.
Highlights: http://www.gao.gov/highlights/d07169high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−07−169

[Return to top]

Information Technology and Telecommunications Sector

38. *December 15, CNET News* — **Yahoo Messenger gets security update.** Yahoo has issued a "highly critical" update for its popular instant messenger feature as it tries to combat security flaws that could allow an attacker to take over a user's system. The flaws affect versions of Yahoo Messenger 5.0 through 8.0, according to a security advisory released Friday, December 15, by Secunia. Windows users who were running versions of Yahoo Messenger before November 2 are advised to update to Yahoo Messenger 8.1.
Secunia Advisory: http://secunia.com/advisories/23401/
Source: http://news.com.com/Yahoo+Messenger+gets+security+update/2100−1002_3−6144110.html?tag=nefd.top

39. *December 15, Tech Web* — **Sturdier botnets mean more spam in 2007.** The late−2006 appearance of durable botnets was a tipping point in the back−and−forth battle against spammers, an industry analyst said Friday, December 15, who predicted that spam will continue to gain ground on defenses. Assembled by a Trojan called SpamThru, the new botnets are tougher to bring down, says Paul Wood, senior analyst with MessageLabs, a message security and filtering service. "The advent of Trojans like SpamThru makes it possible for each bot in the net to learn about the location of other bots. When a bot goes down or the command and control channel is compromised, the other bots know about it." In SpamThru's techniques, if a control server is shut down, the spammer can easily update the rest of the bots with the location of a new server as long as he controls at least one bot in the net. And if a specific bot is shut down, its spam load can be quickly shifted to another, as−yet−undiscovered, bot. "Until now, it's not been possible to regain control of a [compromised] botnet," says Wood. "This

makes botnets much more resilient."
Source: http://www.techweb.com/showArticle.jhtml;jsessionid=4Z3ROB0E0ONAIQSNDLPCKHSCJUNN2JVN?articleID=196700223

40. *December 14, Government Computer News* — **Agencies waiting on vendors for IPv6 security products.** With the deadline to move their network backbone to Internet Protocol Version 6 (IPv6) still about 18 months away, agencies' biggest concern is whether the security industry will have enough products to support them. Three agency officials who are leading efforts to move to IPv6 expressed concern over the lack of support from security vendors so far, and said federal agencies, such as the National Institute of Standards and Technology and the Defense Advanced Research Projects Agency, will have to provide seed money to move products along. "Security has not received the same focus as, say, routers," said John McManus, Commerce Department deputy CIO and co−chairman of the IPv6 working group. "The Office of Management and Budget's memo said the security must be at least the same, if not higher. If you can't secure your network, you will not bring it online."
Source: http://www.gcn.com/online/vol1_no1/42797−1.html

41. *December 14, Government Computer News* — **Intel data protection levels to be standardized.** The federal government is poised to adopt a common array of data protection levels and criteria by which the secrecy rankings are to be determined, according to Dale Meyerrose, CIO of the Office of the Director of National Intelligence. The newly standardized security rankings will replace a patchwork of varying methods the Pentagon, the intelligence community and other agencies have adopted for assuring the technical protection of secret data, Meyerrose said Thursday, December 14, during remarks at an Association for Federal Information Resource Management event. The new set of protection levels and criteria flow from the intelligence community's project to reform certification and accreditation methods. That reform process, which has included an unprecedented level of public involvement, soon will generate a total of seven major changes to federal IT security rules, Meyerrose said. "The particulars of those seven major changes we are still working out, but there are seven major departures from existing security doctrine," Meyerrose said.
Source: http://www.gcn.com/online/vol1_no1/42796−1.html

42. *December 13, IDG News Service* — **Russian expert: Terrorists may try cyberattacks.** A Russian computer security expert predicts that terrorists could seek to target the country's critical infrastructure through electronic warfare, a strategy that could raise the stakes in how Russia handles computer crime. While terrorists aren't believed to currently have the know−how to disrupt critical infrastructure, it would be "very dangerous" if they start learning, said Valery Vasenin, head of the Computer Security Department at the Institute for Information Security Problems at Moscow State University. "I think the phenomenon of terrorism will go in this direction," Vasenin said in an interview at his office. Russia's energy grid is a possible target, which could cause widespread blackouts. The air transportation or fuel distribution systems are other possible targets, Vasenin said. No major cyberterrorism incident in Russia has been recorded. However, the country's infrastructure is becoming more networked and less isolated than before, which could make it more vulnerable to cyberattacks, Vasenin said. "Russia, at the moment, is average in terms of computer security, like the rest of the world," Vasenin said. Russia lacks laws that clearly define computer crime, he said, making it difficult for Internal Affairs Ministry agents to investigate and bring cases.

Source: http://www.infoworld.com/article/06/12/13/HNcyberterroralert_1.html?source=rss&url=http://www.infoworld.com/article/06/12/13/HNcyberterroralert_1.html

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4662 (eDonkey2000), 139 (netbios−ssn), 25 (smtp), 4672 (eMule), 1434 (ms−sql−m), 1433 (ms−sql−s), 1027 (icq), 113 (auth), 135 (epmap) 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

43. *December 13, Arizona Republic* — **Explosive items found in storage unit.** The Glendale, AZ, police bomb squad was called out early Wednesday, December 13, after a number of explosive devices were found inside a storage locker. Bomb technicians remained throughout the morning loading up the devices at Cactus Self Storage. Officer Matt Barnett, a Glendale police spokesperson, said police found "a number of explosive devices" that appear to have been homemade. After the devices were rendered safe for transport, they were taken to a remote area by police escort and then safely detonated, Barnett said. Police were called after managers at the gated business became suspicious about items in an abandoned storage locker.
Source: http://www.azcentral.com/community/glendale/articles/1213brk−explosives1213−ON.html

[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