Department of Homeland Security Daily Open Source Infrastructure Report for 30 November 2005

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

Daily Highlights

- The Albany Democrat−Herald reports the attempted theft of copper wire from a power line knocked out power to 16,568 Pacific Power customers in east Linn County, Oregon, on Monday, November 28. (See item 3)
- The Government Accountability Office has published a report entitled Aviation Security: Federal Air Marshal Service Could Benefit from Improved Planning and Controls, which includes the management of mission−related incidents that affect air marshals' ability to operate discreetly. (See item 8)
- The Associated Press reports Miami police are planning "in−your−face" shows of force in public places, saying the random, high−profile security operations should keep terrorists guessing about where officers might be next. (See item 34)

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. *November 29, Associated Press* — **Snowstorm knocks out power across plains.** Broad areas of the Dakotas remained shut down Tuesday, November 29, by the Plains' first blizzard of the season, with highways closed by blowing, drifting snow and thousands of people without

electricity as temperatures hit the low teens. Utility officials estimated that 50,000 customers were blacked out across eastern South Dakota on Tuesday, and many communities in North Dakota also had no electricity. Power companies in North Dakota said it could take days to restore power because the storm tore down major transmission lines. Utility crews were out early Tuesday working to restore electricity in northwestern Minnesota.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/11/29/AR2005112900095.html

2. *November 29, The Christian Science Monitor* — **Natural gas supplies in much of the U.S. could be affected by cold winter weather.** The eastern half the United States confronts the possibility that harshly cold weather this winter will lead to restrictions of natural gas supplies. In some places −− areas heavily dependent on natural gas to produce electricity −− the prospect of rolling blackouts is much higher than in previous winters. Any natural gas cutoffs would primarily affect electric power plants and factories fueled by gas, not homes, and be most likely in the Northeast. If cold deepens for prolonged periods, the likelihood of interrupted natural gas supplies rises to 30 percent in the Northeast and to 10 percent as far south as Florida and as far west as Missouri, according to a recent report by the Interstate Natural Gas Association of America (INGAA), a trade association representing gas pipeline companies. If winter temperatures plummet for long, natural gas supplies could be quickly depleted, leading to a power crunch in some regions and soaring prices across a wider area, experts say. "By no stretch of the imagination is this only going to impact New England," says energy expert Richard Levitan. "The Southeast, Pennsylvania, New Jersey, Maryland, and New York, they're all going to feel this," said Levitan.
INGAA report: http://www.ingaa.org/Documents/HurricaneRecoveryReport_11−09 −05.pdf
Source: http://www.csmonitor.com/2005/1129/p01s02−usec.html

3. *November 29, Albany Democrat−Herald (OR)* — **Attempted theft leads to power outage.** The attempted theft of copper wire from a power line knocked out power to 16,568 Pacific Power customers in east Linn County, OR, on Monday, November 28, said company spokesperson Doris Johnston. Someone attempted to pull a copper grounding line from a power pole around 10 p.m., said Johnston. Using a vehicle to pull the grounding line, someone pulled the power pole, which carried a transmission line, into a main line, causing the outage. Power was restored within minutes. Police are investigating the incident.
Source: http://www.dhonline.com/articles/2005/11/29/news/local/news0 9.txt

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *November 27, News Channel 5 (OH)* — **Ammonia leak forces residents from homes in Ohio.** An ammonia leak forced residents from their homes in Wadsworth in Medina County, OH, Sunday, November 27. Officers said 50 people had to be evacuated from their homes at about 1 p.m. EST after a leak was found coming from a downtown business. Police, fire and Hazmat teams responded, found the leak and immediately worked to repair the line. Wadsworth Fire Chief Ralph Copley said it a weak spot in one of the lines was to blame for the leak.
Source: http://www.newsnet5.com/news/5412609/detail.html

[Return to top]

Defense Industrial Base Sector

5. *November 29, Defense Industry Daily* — **Canada unveils national aerospace industry strategy.** The Canadian government has released the National Aerospace and Defense Strategic Framework, a 20−year vision aimed at helping Canada's leaders in the aerospace, defense and space sectors identify where and how they can be globally competitive. The document is the result of the Canadian Aerospace Partnership process that began in April 2005 among industry, regional and national government, academia, and labor. The report addresses both global aerospace industry trends, and matters specific to Canada's situation. A strength listed for the industry in Canada is its ties to U.S. industry via agreements, subsidiaries, and geography. Over the past 10 years, more than 70 percent of Canada's aerospace exports have gone to the U.S. National Aerospace and Defense Strategic Framework: http://strategis.ic.gc.ca/epic/internet/inad−ad.nsf/vwapj/ae rospace−e.pdf/$file/aerospace−e.pdf Source: http://www.defenseindustrydaily.com/2005/11/canada−unveils−national−aerospace−industry−strategy/index.php#more

[Return to top]

Banking and Finance Sector

6. *November 29, Finextra Research* — **Online brokerage affected by computer hacker.** Online brokerage Scottrade is warning customers that their personal financial details may have been compromised due to a security breach at its e−payments services provider Troy Group. Scottrade has not disclosed how many of its 1.3 million customers had been affected, but it says the breach mainly affects clients who use its eCheck Secure service to transfer funds from their bank account to their online brokerage accounts. California−based Troy Group reported on October 25 that a computer hacker had compromised its e−Check servers and that it had filed a report of the crime with the FBI. In a letter to customers, Scottrade says as a result of the breach “some of your personal information, including your name, driver's license or state ID number, date of birth, phone number, bank name, bank code, bank number, bank routing number, bank account number and Scottrade account number may have been compromised.” Last month Scottrade said it was implementing two−way two−factor authentication technology in a bid to protect its customers from Internet fraud and identity theft.
Source: http://www.finextra.com/fullstory.asp?id=14584

7. *October 24, Government Accountability Office* — **GAO−06−19: Terrorist Financing: Better Strategic Planning Needed to Coordinate U.S. Efforts to Deliver Counter−Terrorism Financing Training and Technical Assistance Abroad (Report).** Terrorist groups need significant amounts of money to organize, recruit, train, and equip adherents. U.S. disruption of terrorist financing can raise the costs and risks and impede their success. This report (1) provides an overview of U.S. government efforts to combat terrorist financing abroad and (2) examines U.S. government efforts to coordinate training and technical assistance. The Government Accountability Office (GAO) also examined specific accountability issues the

Department of the Treasury faces in its efforts to block terrorists' assets held under U.S. jurisdiction. GAO recommends that the Secretaries of State and the Treasury implement an integrated strategic plan and a Memorandum of Agreement for the delivery of training and technical assistance. Congress should also consider requiring the Secretaries of State and the Treasury to report the status of that implementation. State disagreed with our recommendations for an integrated strategy and Memorandum of Agreement. Treasury did not directly address these recommendations. While Treasury did not disagree with implementing an integrated strategic plan, it limited the plan's coverage to priority countries. GAO makes additional recommendations to Treasury concerning Treasury's terrorist asset blocking efforts with which Treasury did not agree.
Highlights: http://www.gao.gov/highlights/d0619high.pdf
Source: http://www.gao.gov/new.items/d0619.pdf

[Return to top]

Transportation and Border Security Sector

8. *November 29, Government Accountability Office* — **GAO−06−203: Aviation Security: Federal Air Marshal Service Could Benefit from Improved Planning and Controls (Report).** The U.S. Federal Air Marshal Service (FAMS) has undergone a number of changes in recent years, including a 2003 transfer from the Transportation Security Administration (TSA) to the U.S. Immigration and Customs Enforcement Bureau (ICE), and a 2005 transfer from ICE back to TSA. A key aspect of federal air marshals' operating procedures is the discreet movement through airports as they check in for their flight, transit−screening checkpoints, and board the aircraft. This report discusses FAMS's (1) transfer to ICE and key practices that could facilitate its return to TSA, and (2) management of mission−related incidents that affect air marshals' ability to operate discreetly. The Government Accountability Office (GAO) recommends that the Secretary of the Department of Homeland Security (DHS) adopt key practices for successful mergers and transformations, to include developing an overall strategy with implementation goals and milestones and a communication strategy. GAO is also recommending that the Secretary direct FAMS to improve management controls for recording, tracking, and addressing mission incidents and communicating the outcome of actions taken to address them. DHS reviewed a draft of this report and agreed with GAO's findings and recommendations.
Highlights: http://www.gao.gov/highlights/d06203high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−203

9. *November 29, Associated Press* — **Delta CFO says $3 billion turnaround plan needed for airline's survival.** Delta Air Lines, which lost $2.6 billion in the first nine months of this year, needs the $3 billion in annual cost savings from its reorganization plan to survive, chief financial officer Edward Bastian told a bankruptcy court on Monday, November 28. "In my opinion it (the cost reduction plan) is absolutely necessary," Bastian told the court during the third day of a hearing on a Delta request to void its contract with pilots and impose $325 million in wage cuts. The Air Line Pilots Association, the union representing the pilots, has offered $90.7 million in concessions and has threatened a strike if the court grants Delta's request. Atlanta−based Delta is seeking cuts from its pilots to help offset rising fuel costs and the impact of stiff competition from low−fare competitors. Delta, which filed for Chapter 11 on

September 14, has recorded losses of more than $11 billion since January 2001. Bastian said the airline is also trying to cut costs by renegotiating aircraft leases, but said its employment costs are hobbling its ability to compete.
Source: http://www.usatoday.com/travel/news/2005−11−28−delta−bankrup tcy_x.htm

10. *November 29, New York Times* — **Federal Aviation Administration calls for mediation in talks with controllers.** Seeking concessions like those that airlines got from pilots, the head of the Federal Aviation Administration called Monday, November 28, for mediation in talks with unionized air traffic controllers, saying contract discussions were near an impasse. The agency's administrator, Marion C. Blakey, said at a news conference that the union was calling for pay increases of 5.6 percent a year for five years, a proposal that Blakey said was out of touch with "the hard reality of an industry that's in real financial trouble." She said her agency, whose biggest revenue source is a tax on plane tickets, was proposing a five−year pay freeze. A strike now does not seem likely, but experts say something as simple as controllers' strict adherence to air traffic rules could create heavy travel delays.
Source: http://www.nytimes.com/2005/11/29/politics/29air.html?pagewa nted=all

11. *November 29, CBC News (Canada)* — **Window broken on board Air Labrador flight.** The Canadian Transportation Safety Board is investigating a weekend incident that the airline says was a case of air rage, but a passenger says was an accident that followed a flight in extremely turbulent winds. Ward Pike, an Air Labrador executive, said the incident on the Twin Otter happened on the runway at Happy Valley−Goose Bay. "An unruly passenger acted in a violent manner and kicked out a window on board the aircraft," Pike said. But passenger Shirley Flowers said she saw nothing fitting that description. She said a passenger accidentally bumped one of the windows with his hand, and it broke. Flowers said the plane had flown through extremely turbulent conditions near the coastal community of Rigolet, before heading to Happy Valley−Goose Bay.
Source: http://www.cbc.ca/story/canada/national/2005/11/29/nfld_airi ncident051129.html

12. *November 29, Detroit Free Press* — **Power problem closes Detroit−Windsor Tunnel.** A problem with an air system at a DTE Energy station in Detroit caused a brief power outage on Tuesday, November 29, that spread from the Detroit−Windsor Tunnel all the way to neighborhoods on the eastside of the city. The outage briefly shut down the Detroit−Windsor Tunnel, which connects the United States to Canada, for more than two and a half hours and cars that couldn’t get though the tunnel were directed to the Ambassador Bridge, officials said.
Source: http://www.freep.com/apps/pbcs.dll/article?AID=/20051129/NEW S11/51129010/1013

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

13. *November 29, Billings Gazette (WY)* — **Chronic wasting disease in third new hunt area in Wyoming.** Two mule deer collected from hunt area 37 near the Bighorn River in Wyoming have tested positive for chronic wasting disease (CWD). This is the third new CWD positive hunt area discovery in the Thermopolis, WY, area this fall. The Game and Fish Department began collecting additional deer samples on Wednesday, November 16, after a sick deer collected near the Wedding of the Waters in hunt area 120 tested positive for CWD. According to Cody wildlife supervisor Gary Brown, this is the first time management action aimed at determining the extent of CWD in an area resulted in identifying a new CWD area. "We collected 28 mule deer from within a one−mile radius of the sick deer's location in adjacent hunt area 37 south of Thermopolis. Two does tested positive for CWD," he said. According to Brown, the Department will collect an additional 22 deer south of Thermopolis in hunt area 120 beginning Thursday, December 1.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2005/11/29/build/wyoming/96−cwd.inc

14. *November 28, United Press International* — **Shade trees being hurt by plant disease.** Plant pathologists with the St. Paul, MN−based, American Phytopathological Society say the plant disease known as bacterial leaf scorch (BLS) affects such shade tree species as the American elm, red maple, sweet gum, sycamore, and several oak species. The disease has been found in street plantings, small woodlots, and landscapes across the eastern United States, as far west as Texas. Ann Brooks Gould, associate extension specialist at Rutgers University, says current loss of value plus replacement costs for older trees affected by the disease is about $8,000 per tree. BLS is caused by a bacterial pathogen, Xylella fastidiosa, which is spread by insects. Symptoms of BLS are similar to those caused by environmental stresses, resulting in the disease being often overlooked or misdiagnosed. According to Gould, management options of BLS in urban trees include maintaining plant vigor, removing infected trees and branches that have died from the disease, avoiding planting highly susceptible trees, and designing new tree plantings with a diverse complement of species.
Source: http://www.upi.com/NewsTrack/view.php?StoryID=20051128−12331 1−4063r

15. *November 28, Western Farm Press* — **Wider, wetter beds linked to lettuce drop.** Research on lettuce drop caused by Sclerotinia species in California fields indicates that plantings on 80−inch beds irrigated twice a week are at greater risk of the fungal disease, says a University of California plant pathologist. Krishna Subbarao observed 40− and 80−inch bed configurations in the Imperial Valley this year and the previous two seasons. Sclerotinia minor is most common in lettuce along the coast, while S. sclerotiorum occurs more often in interior valleys. Under wet conditions, both pathogens attack the lower leaves and stems, leading to decay which collapses plants nearing maturity. “Results obtained thus far...clearly indicate the potential for 80−inch beds to increase lettuce drop incidence caused by both species. This, in turn, can lead to greater numbers of sclerotia in the soil and the establishment of the airborne phase of S. sclerotiorum in the Salinas Valley,” Subbarao said. The 80−inch bed concept, which requires custom−built, wider equipment, has been adopted by several farming operations as a means of reducing labor and tractor costs and soil compaction.
Source: http://westernfarmpress.com/news/11−28−05−beds−linked−to−let tuce−drop/

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

16. *November 29, Journal Star (NE)* — **Water debt threatening a way of life.** Nebraska hasn't been living up to the terms of its agreement to give Kansas 40 percent of the flow of the Republican River, as it agreed to do in a 2002 settlement to a lawsuit. As drought gripped the state, Nebraska failed to live up to its agreement in 2003 and again in 2004. By the end of this year, Nebraska will owe Kansas more than 100,000 acre−feet of water. An acre−foot is the amount of water needed to cover one acre to a depth of one foot. If Nebraska stopped irrigating 100,000 acres in the basin for three years, it still wouldn't solve the problem, according to water officials. Last year, the Lower Republican Natural Resources District cut back pumping by 25 percent. But it hasn't been enough. Under the settlement, Nebraska can use a five−year average in measuring water supplied to Kansas. In the meantime, irrigators and officials are desperately searching for a way to come up with the water Nebraska owes Kansas. A new federal program, partially funded by the state, pays farmers to take land out of irrigation, but there's uncertainty about whether the state's taxpayers are willing to expand the program.
Source: http://www.journalstar.com/articles/2005/11/29/editorial_main/doc438baa56a0e4d570303933.txt

[Return to top]

Public Health Sector

17. *November 29, Agence France Presse* — **Bird flu subsides in Russia.** Outbreaks of bird flu have subsided in Russia and the virus is now known to be present in only two locations in the country, a sharp decrease from the 10 zones that were affected a month ago. "As of November 29, there are still two areas on the territory of the Russian Federation affected by bird flu," the health ministry said in a statement. One was in the region of Kurgan about 1,300 miles southeast of Moscow and the other in the Astrakhan region 930 miles south of the capital on the edge of the Caspian Sea, the ministry said.
Source: http://news.yahoo.com/s/afp/20051129/hl_afp/healthflurussia_051129130010;_ylt=AnPOANbVz6UvPtZpGNIOELWJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

18. *November 29, Proceedings of the National Academy of Sciences* — **Genome sequence of Clostridium botulinum type C neurotoxin−converting phage.** Botulinum neurotoxins (BoNTXs) produced by Clostridium botulinum are among the most poisonous substances known. Of the seven types of BoNTXs, genes for type C1 and D toxins (BoNTX/C1 and D) are carried by bacteriophages. The gene for exoenzyme C3 also resides on these phages. Researchers present the complete genome sequence of c−st, a representative of BoNTX/C1−converting phages. The genome is a linear double−stranded DNA of 185,682 bp with 404−bp terminal direct repeats, the largest known temperate phage genome. Researchers

identified 198 potential protein−coding regions, including the genes for production of BoNTX/C1 and exoenzyme C3. Very exceptionally, as a viable bacteriophage, a number of insertion sequences were found on the c−st genome. By analyzing the molecular structure of the c−st genome in lysogens, researchers also found that it exists as a circular plasmid prophage. These features account for the unstable lysogeny of BoNTX phages, which has historically been called "pseudolysogeny." The PCR scanning analysis of other BoNTX/C1 and D phages based on the c−st sequence further revealed that BoNTX phages comprise a divergent phage family, probably generated by exchanging genomic segments among BoNTX phages and their relatives.
Source: http://www.pnas.org/cgi/content/full/102/48/17472

19. *November 28, Stockholm University (Sweden)* — **Researchers discover substance that may stop anthrax bacteria.** Researchers at Stockholm University have found a substance that quickly knocks out the anthrax bacterium. The scientists have identified the enzyme in the bacterium that makes it multiply. The substance N−hydroxylamine arrests the enzyme, and the bacterium stops growing. “An anthrax infection in the lungs develops very rapidly and must be stopped as quickly as possible. This can be done by combining the substance N−hydroxylamine with ordinary antibiotics that work more slowly,” said Professor Britt−Marie Sjöberg, Department of Molecular Biology and Functional Genomics. “The fact that we have identified a chemically simple and commercially available substance with these properties is of great significance both practically and in terms of further research,” added Sjöberg.
Source: http://www.su.se/pub/jsp/polopoly.jsp?d=1043&a=3725

20. *November 28, CIDRAP* — **Many H5N1 cases bunched in families.** More than a third of the human cases of H5N1 avian influenza that occurred over a 19−month period were clustered within families, suggesting the possibility that some family members caught the virus from others, according to a recent report. Forty−one of 109 cases identified between January 2004 and July 2005 occurred in 15 families, with between two and five cases per family, according to the report. Researchers previously identified one cluster, involving a young Thai girl and her mother and aunt in September 2004, as a probable result of person−to−person transmission. Too little information is available to conclude whether the virus spread from person to person in any of the other families. Family clusters don't necessarily mean the virus is spreading from person to person, the report notes. They may simply mean that relatives were exposed to H5N1−infected poultry at the same time. However, in three family clusters, the first and second patients fell ill more than a week apart, which suggests that they probably didn't acquire the virus from the same source at the same time.
Report: http://www.cdc.gov/ncidod/EID/vol11no11/05−0646.htm
Source: http://www.cidrap.umn.edu/cidrap/content/influenza/avianflu/news/nov2805family.html

21. *November 28, Associated Press* — **Study: Bird flu vaccine can stop spread.** Vaccines can keep chickens from dying of bird flu, but can immunized birds still silently spread infection? Scientists in the Netherlands put the question to a test −− using vaccines against a different strain −− and concluded that vaccinating poultry indeed can block viral spread between birds. "Vaccination can be an attractive tool to prevent outbreaks of highly pathogenic AI (avian influenza) viruses in poultry, thereby achieving the aim of eliminating the source of human infections," concludes lead researcher J.A. van der Groot of the Netherlands' Central Institute

for Animal Disease Control. Previous research found that vaccination could protect individual chickens from falling ill with various flu strains. But there have been reports of asymptomatic chickens shedding virus after vaccination, raising concern. So van der Groot and colleagues tested two vaccines against the H7N7 bird−flu strain, by housing infected chickens together with healthy vaccinated ones. Two weeks after inoculation, both vaccines completely blocked H7N7 spread between chickens. There were marginal differences in effectiveness between the two vaccines, however, leading the researchers to conclude that poultry vaccines' ability to stop viral spread should be tested before health authorities choose which one to use.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/11/28/AR2005112801160.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *November 29, Daily Yomiuri Online (Japan)* — **Japanese antiterror drill not foolproof, reveals flaws in response plan.** An exercise conducted in Fukui Prefecture, Japan, on Sunday, November 27, simulating a terrorist attack on a nuclear power plant has brought to the fore a host of problems that must be resolved to boost the nation's emergency preparedness. Although the exercise went as planned, it failed to answer several questions that must be addressed to ensure evacuation operations could be successfully implemented in a real terrorist attack. The exercise was conducted on the Tsuruga Peninsula, which has many sightseeing spots and is packed with beachgoers and other tourists in the summer. However, how to evacuate these sightseers safely was not considered in this exercise. In addition, one impediment expected to hamper evacuations and antiterrorist activities is road congestion. The prefecture's two major highways linking the peninsula with the Hokuriku Expressway are often jam−packed with vehicles, especially in the summer. One key measure to prevent traffic jams in the exercise involved local authorities calling on residents to walk to designated assembly spots. In addition, some officials who took part in the exercise said discrepancies among different organizations involved in the evacuation that use markedly different designations and equipment needed to be resolved.
Source: http://www.yomiuri.co.jp/dy/national/20051129TDY03004.htm

23. *November 28, Associated Press* — **Authorities stage anti−terror drill at Florence's Pitti Palace.** Italian authorities staged a terrorism drill in Florence's Pitti Palace on Monday, November 28, simulating a nerve gas attack in a gallery housing paintings by Titian, Raphael and Caravaggio. The drill, the latest in a series of similar exercises held in major Italian cities over the past months, involved about 400 people, the prefect's office in Florence said. It was designed to test the city's response and the coordination between law enforcement officials and emergency workers in case of a major attack. The Pitti Palace, dating to the 15th century, is a massive, golden−colored building in the heart of Florence. The museum where the drill was

staged, the "Galleria Palatina," houses some 500 paintings, and is a major tourist attraction in the city. Italy has been on high alert since the July 7 terror attacks in London. Cities that have staged anti−terror drills include Rome, Milan and Turin, where winter Olympics are scheduled to be held early next year.
Source: http://msnbc.msn.com/id/10236636/

24. *November 28, St. Louis Post−Dispatch (MO)* — **Group urges more disaster planning in Missouri.** Downtown St. Louis, MO, is better prepared for disasters than four years ago due to the cooperative effort among businesses and public safety agencies, leaders of the effort said Monday, November 28. Former Senator John C. Danforth (R−MO) and St. Louis lawyer Walter Metcalfe spoke about enlisting more partners in making plans to deal with a range of possibilities including earthquakes, tornadoes, terrorist attacks or chemical leaks. Danforth and Metcalfe head the Downtown St. Louis Emergency Preparedness Organization, a nonprofit public and private partnership known as DSTEP. The group is seeking to identify needs and supply resources to assure that downtown will be prepared in the event of a public emergency, as well as improve communication between first responders and downtown businesses and residents. "Preparedness is everything, communications is everything," said Danforth at a news conference, noting that the group was formed after the attacks of September 11, 2001. The group already has 55 members −− representing businesses, buildings, agencies and organizations −− who are participating in a dedicated radio communication system linking them directly to police and fire departments.
Source: http://www.stltoday.com/stltoday/news/stories.nsf/stlouiscityco unty/story/825D444D142642E3862570C8001739B9?OpenDocument

[Return to top]

Information Technology and Telecommunications Sector

25. *November 29, Security Focus* — **Microsoft Windows SynAttackProtect predictable hash remote denial of service vulnerability.** Microsoft Windows is prone to a denial of service vulnerability. The vulnerability arises due to a design error in the function responsible for the hash table management for "SynAttackProtect." Reports indicate that the affected function used by the TCP/IP stack creates a predictable hash, allowing an attacker to send a large number of SYN packets with an identical hash value. A successful attack can eventually lead to a denial of service condition due to the lookup algorithm becoming very inefficient at performing searches.
Solution: http://www.securityfocus.com/bid/15613/solution
Source: http://www.securityfocus.com/bid/15613/references

26. *November 29, Associated Press* — **Deadline passes for Internet phone service.** Vonage Holdings Corp., the nation's largest non−cable provider of Internet phone service, could be barred from signing up new customers in many markets because it failed to meet the deadline to provide reliable emergency 911 service to all subscribers. The Federal Communications Commission (FCC) gave Vonage and other companies that sell Internet−based phone service 120 days to comply with its order requiring enhanced 911, or E911, in all their service areas. The deadline to show the government where E911 is available was Monday, November 28. Citing public safety concerns, the FCC in May ordered companies selling Voice over Internet Protocol (VoIP) to ensure that callers can reach an emergency dispatcher when they dial 911.

The dispatchers also must be able to tell where callers are located and the numbers from which they are calling. VoIP providers were told that if they failed to meet the deadline they could no longer market their service or accept new customers in areas that didn't have enhanced 911. They will not have to disconnect current customers who don't have full 911 service, as some providers had feared.
Source: http://news.yahoo.com/s/ap/20051129/ap_on_hi_te/internet_phones_e911;_ylt=AjaLT2jsjEo3.4v7erjRrDcjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

27. *November 28, Government Computer News* — **Controls on Federal Bureau of Investigation Sentinel project paying off, inspector general says.** Although the Federal Bureau of Investigation (FBI) experienced a major setback in its failure to deploy the long−awaited Virtual Case File (VCF) IT system, it is performing better in its management of the Sentinel successor system, according to a report from the Department of Justice's inspector general. Because of the serious problems with development of the VCF project −− which was to replace the FBI's paper−based criminal investigation records system with electronic records −− the inspector general's office said it has initiated a long−term audit and continued monitoring of Sentinel, and will issue several reports on the project in the coming months. There are signs of improvement. "As of October 2005, our preliminary assessment is that the FBI has instituted important improvements in its IT management controls and practices that it did not have when it attempted to develop the Virtual Case File," the inspector general's report said. The report highlights several major management challenges at the department, including concerns about timely upgrades to IT systems, information−sharing and information security. Despite some successes the FBI's current IT systems overall "fall far short of what is needed," the report concluded.
Department of Justice report: http://www.usdoj.gov/oig/challenges/2005.htm
Additional information on Sentinel: http://www.gcn.com/24_12/news/35886−1.html
Source: http://www.gcn.com/vol1_no1/daily−updates/37653−1.html

28. *November 28, Reuters* — **Federal Trade Commission: Spam e−mail filters getting better.** E−mail spammers are aggressive as ever but Internet providers are getting better at blocking junk messages before they reach users' inboxes, according to a U.S. Federal Trade Commission (FTC) study released on Monday, November 28. The FTC found that spammers continue to "scrape" e−mail addresses from the Web using automated programs that look for the telltale "@" sign. But up to 96 percent of those messages were blocked by the two Web−based e−mail providers used by the FTC in its test. The FTC did not say which providers it used in its study. "This encouraging result suggests that anti−spam technologies may be dramatically reducing the burden of spam on consumers," the report said. The FTC noted that Internet providers still must bear the burden of filtering out those messages.
FTC Press Release: http://www.ftc.gov/opa/2005/11/spam3.htm
FTC Spam study: http://www.ftc.gov/opa/2005/11/spamharvest.pdf
Source: http://today.reuters.com/news/NewsArticle.aspx?type=internetNews&storyID=2005−11−28T211837Z_01_SPI876594_RTRUKOC_0_US−SP AM.xml

29. *November 28, Government Computer News* — **Agencies must monitor insider network threats, expert says.** Agency networks are more vulnerable than ever, according to a former Central Intelligence Agency (CIA) official and cybersecurity expert, and the greatest threat to

an organization's network security may come from within. Eric Cole, who worked for the CIA for more than five years, told an audience of government and corporate security professionals Monday, November 28, at the inaugural Techno Forensics Conference at the National Institute of Standards and Technology that despite their best efforts, networks are only getting more porous. Cole said an emerging threat for organizations is that the emphasis on thwarting outside attacks and tracing their origins has led them to overlook the insider threat. In several recent cases, organizations conducted preliminary forensic examinations after network incidents and identified employees as being responsible. Aside from network insecurity, Cole said agencies need to have standardized procedures for computer forensics. A lack of standardized procedures for computer forensics, he warned, will jeopardize organizations' abilities to use forensic examinations at trial.
Source: http://www.gcn.com/vol1_no1/daily−updates/37654−1.html

30. *November 28, eWeek* — **Malicious keyloggers run rampant on net.** Keylogging programs are the epitome of online stealth, and they're also a mushrooming problem on the Internet. Reports of new keylogging programs soared higher this year, as part of a wave of multifunction malware with integrated keylogging features, according to VeriSign Inc.'s security information company iDefense Inc. The programs often evade detection by anti−virus tools and can be difficult to detect once installed, experts warn. More than 6,000 keylogging programs will be released by the end of this year, according to projections by iDefense. That's an increase of 2,000 percent over the last five years, company officials said. Keyloggers have been around for years and are also sold as legitimate applications −− often as monitoring tools for concerned parents or suspicious spouses −− according to Ken Dunham, director of malicious code at iDefense, in Reston, VA. Malicious keyloggers are increasingly part of modular programs that contain Trojan horse, spamming and remote control features, as well, Dunham said. Anti−virus companies have developed signatures that will stop many of those programs before they can be installed, but new programs with unique signatures are readily available from malicious code download sites.
Source: http://www.eweek.com/article2/0,1895,1893515,00.asp

31. *November 25, Reuters* — **European Union committee backs telecom data storage rule.** A European Union (EU) committee agreed that details of all EU−wide phone calls and Internet use should be stored, but the steps did not go as far as some member states had wanted in the battle against terrorism and crime. The European Parliament's civil liberties committee voted by 33 to eight in favor of the new rules on Thursday, November 24, whereby details on telephone calls and Internet use −− but not their content −− would be kept for six to 12 months. Telecom firms typically store data for three months for billing purposes. Some EU states want it kept for 24 months. The full Parliament votes on the rules in December, and member states must approve them before they become law.
Source: http://today.reuters.com/news/newsArticleSearch.aspx?storyID=85494+25−Nov−2005+RTRS&srch=eu+data+storage+rule

32. *November 21, Federal Computer Weekly* — **Lost records convince officials that encrypted digital backups are crucial.** After Hurricane Katrina devastated the Gulf Coast region, along with many vital records, federal officials realized they needed to digitize such records to prevent future data loss. But storage analysts say federal agencies are behind the curve when it comes to safeguarding digitized records stored elsewhere. Federal agencies are not encrypting

their off−site data, said Jon Oltsik, a senior analyst at research firm Enterprise Strategy Group. Katrina's destruction demonstrated the importance of electronic backup copies of documents such as health records and flood maps. But by keeping copies of critical information, agencies also create new opportunities for data theft. Oltsik is the author of a recent survey that asked 388 agencies and companies whether they encrypt backup data as they copy it to tape. "Of the five industry segments we looked at, [the local/federal] government was the worst," he said. Only three percent of government organizations said they always encrypt backup data, and 77 percent said they never do. Overall, only seven percent of the organizations surveyed said they always encrypt backup data, despite the fact that vendors have offered backup encryption tools for at least 15 years, Oltsik said.
Source: http://fcw.com/article91509−11−21−05−Print

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

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

US−CERT Operations Center Synopsis: US−CERT is aware of a publicly reported vulnerability in the way Cisco PIX firewalls process legitimate TCP connection attempts. A remote attacker may be able to send spoofed, malformed TCP packets with incorrect checksum values through affected PIX firewalls. Legitimate network traffic to the destination, PIX protected hosts may be blocked until the invalid PIX connection attempt entry times out around two minutes by default. Until a patch or more information becomes available,
US−CERT recommends that system administrators who may be affected consider reconfiguring certain connection timers on Cisco PIX systems.Public exploit code for this reported vulnerability may be useful for automating a sustained attack.

For more information please review the following US−CERT Vulnerability Note (VU#853540):
Cisco PIX TCP checksum verification failure report
http://www.kb.cert.org/vuls/id/853540

Current Port Attacks

Top 10 Target Ports	17651 (−−−), 6881 (bittorrent), 1026 (win−rpc), 445 (microsoft−ds), 80 (www), 27015 (halflife), 1029 (−−−), 50202 (−−−), 65535 (Adoreworm), 53 (domain) 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

33. *November 29, New York Daily News* — **Odor sends school into panic.** Ambulances rushed dozens of students and adults from Center Moriches High School in Center Noriches, Long Island, to area hospitals on Monday, November 28, after the group reported feeling ill due to an odor in a classroom. A chaotic scene, which included the evacuation of the Frowein Road school, was further complicated when a female student suffered an unrelated seizure just as paramedics arrived at the building, police said. Nineteen students, three food workers and two teachers −− whose symptoms were mainly dizziness and headaches −− were treated and released from the hospital. Air quality tests showed nothing to explain the illnesses, Center Moriches schools Superintendent Donald James said "Please be aware that every precaution was taken by the school district to ensure student safety," James said in a prepared statement. "There have been no medical findings confirming any carbon monoxide poisoning or any other environmentally related matters pertaining to the illnesses."
Source: http://www.nydailynews.com/boroughs/story/369770p−314615c.ht ml

34. *November 29, Associated Press* — **Miami police take new tack against terror.** Police are planning "in−your−face" shows of force in public places, saying the random, high−profile security operations will keep terrorists guessing about where officers might be next. As an example, uniformed and plainclothes officers might surround a bank building unannounced, contact the manager about ways to be vigilant against terrorists and hand out leaflets in three languages to customers and people passing by, said police spokesperson Angel Calzadilla. He said there would be no random checks of identification. The operations will keep terrorists off guard, Fernandez said. He said al Qaeda and other terrorist groups plot attacks by putting places under surveillance and watching for flaws and patterns in security. Police Chief John Timoney said there was no specific, credible threat of an imminent terror attack in Miami. But he said the city has repeatedly been mentioned in intelligence reports as a potential target. Under the program, both uniformed and plainclothes police will ride buses and trains, while others will conduct longer−term surveillance operations. Mary Ann Viverette, president of the International Association of Chiefs of Police, said the Miami program is similar to those used for years during the holiday season to deter criminals at busy places such as shopping malls.
Source: http://www.cbsnews.com/stories/2005/11/29/ap/national/mainD8 E68RL82.shtml

[Return to top]

General Sector

35. *November 28, eWeek* — **European Commission tightens database ties to fight terrorism.** The European Commission (EC) last week adopted measures that will help fight terrorism and serious crime by opening up development of, and access to, common databases. The databases in question are the VIS (Visa Information System), the SIS (Schengen Information System) and EURODAC (a database containing fingerprints of asylum seekers and illegal immigrants). One of the adopted proposals grants access to the VIS database to both member states responsible for internal security as well as to Europol as they seek to prevent, detect and investigate terrorist offenses and other serious crimes. In order to ensure both the free movement of individuals as well as a high level of security, the EC has given top priority to developing the VIS database as

a system to exchange visa data between Member States. The EC is also considering initiatives such as establishing a system to monitor entry and exit, as well as a system to make it easier for frequent travelers to cross external borders.
Source: http://www.eweek.com/article2/0,1895,1893687,00.asp

[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