Department of Homeland Security Daily Open Source Infrastructure Report for 09 November 2005

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

Daily Highlights

- The News & Observer reports someone placed a large black flag atop a communications tower on the grounds of the Shearon Harris Nuclear Plant in southwest Wake County, North Carolina, last week. (See item 4)
- The Arizona Daily Star reports 17 Tucson, Arizona−area residents were indicted on charges of using stolen credit and debit card numbers and other personal information to steal money from ATMs as part of an international computer−based theft ring. (See item 8)
- The Associated Press reports the U.S. has proposed that the United Nations health agency immediately convene a small expert group to plan a rapid response in the event of a flu pandemic. (See item 18)
- The US−CERT has released "Technical Cyber Security Alert TA05−312A: Microsoft Windows Image Processing Vulnerabilities." (See item 27)

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 08, Energy Information Administration — **Gulf hurricane damage still impacting energy outlook according to government report.** The Energy Information Administration has released its latest Short−Term Energy Outlook, taking into consideration the impact of Hurricanes Katrina and Rita. The hurricanes damaged, set adrift, or sunk 192 oil and natural gas drilling rigs and producing platforms, causing significant damage to the U.S. petroleum and natural gas industries. At the beginning of November almost 53 percent of normal daily Federal Gulf of Mexico oil production and 47 percent of Federal Gulf of Mexico natural gas production remains shut in. Some wells were temporarily shut in as a precaution to Hurricane Wilma. While no damage was reported from that storm, hurricane recovery remains a key factor in this Outlook. Recent information on damaged and destroyed platforms and shut−in production suggests that the recovery path will be slower than predicted in the October Outlook. This short−term forecast projects that total energy demand is likely to respond to higher prices and hurricane−related destruction by showing relatively flat growth between 2004 and 2005, compared with 1.5−percent growth between 2003 and 2004. However, energy demand is expected to recover in 2006 at a rate of about two percent.
Source: http://www.eia.doe.gov/steo

2. *November 07, Associated Press* — **Tire shortage causes problems for coal mines.** Coal mining companies in the Powder River Basin in northeast Wyoming are maneuvering to get around a worldwide shortage of tires for heavy equipment. The shortage is widely attributed to increasing demand from U.S. and international mining operations for tires, industry officials said. Military operations in Iraq and Afghanistan have added to the strain on the tire market, said Jim Davis, a Goodyear Tire & Rubber Co. spokesperson. Drivers and mechanics at Wyoming mines are getting instructions intended to extend the life of off−the−road tires used on the giant dump trucks used to haul overburden and coal. Companies are also scrambling to make up the shortage through deals with suppliers, which are so tightly strapped that at least one mine has had to idle some of its trucks in recent weeks. To meet the demand, manufacturers like Goodyear and Bridgestone Corp. are looking at expanding the capacity of their big tire plants. Davis said the heavy−equipment tire shortage could continue through 2007.
Source: http://www.grandforks.com/mld/grandforks/news/state/13105832 .htm

3. *November 07, Pacific Business News* — **Utility warns of tight power supply.** Hawaiian Electric Co. (HECO) has asked some of its biggest customers to reduce electricity use because six of 19 power generating units on Oahu are shut down or running below capacity. HECO also is asking residential customers to conserve power by turning off air conditioning and postponing the use of big appliances until later in the evening. The utility said it experienced problems with several power generating units over the weekend, in addition to units that had already been taken down for repairs and maintenance. Also, the H−Power waste−to−energy plant is operating at reduced power because of mechanical problems. HECO spokesperson Jose Dizon said repairs are under way but said it could take the rest of the week for all of the power−generating capacity to be restored.
Source: http://www.bizjournals.com/pacific/stories/2005/11/07/daily5 .html?from_rss=1

4. *November 07, News & Observer (NC)* — **Black flag found at nuclear plant.** Someone placed a large black flag atop a communications tower on the grounds of the Shearon Harris Nuclear Plant in southwest Wake County last week, a Progress Energy official said Monday, November 7. Plant security officers discovered the 5−foot by 8−foot flag during a patrol about 8 a.m. EST

Friday, November 4, said Julie Hans, a spokesperson for Progress Energy. The tower, which has phone and Internet connections for the plant, is nearly a mile from the secured area, which is protected with fences and security personnel. The flag was hung about 75 feet up the 100−foot tower. The plant contacted law enforcement and the U.S. Nuclear Regulatory Commission (NRC). "Our site security personnel are working with the Wake County sheriff's department and the FBI on the investigation," Hans said. "There were no threats made. There was no note left. Just a black flag," said Hans. "It appears to have been a prank," said Ken Clark, a spokesperson for the NRC in Atlanta. "The area is owner controlled and patrolled, but it is not fenced off and not vital to the defense of the plant," said Clark. The plant is located near Raleigh, NC.
Source: http://newsobserver.com/news/story/2833641p−9284292c.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *November 07, Chippewa Herald (WI)* — **Tanker flips, spills gasoline, closing parts of two Wisconsin highways.** A tanker truck filled with more than 8,000 gallons of gasoline rolled into a ditch near Chippewa, WI, along Highway 29 near Highway 53 on Sunday, November 6, closing parts of the two highways for more than six hours and putting into potential danger residents and shoppers within a half−mile of the area. The truck went off the road around 6 a.m. and rolled down a steep embankment along Highway 29 West on the exit ramp to Highway 53 North. After disengaging from the cab, the trailer rolled down an embankment, puncturing its tanks, causing gasoline to leak. The driver suffered broken ribs and other minor injuries. Excessive speed was attributed to the cause of the accident.
Source: http://www.chippewa.com/articles/2005/11/07/news/news1.prt

[Return to top]

Defense Industrial Base Sector

6. *November 07, Agence France−Presse* — **U.S. lifts ban on Israeli involvement in new jet fighter.** The United States will allow Israel to help develop the next generation Joint Strike Fighter jet following a disagreement over arms sales to China, according to Israeli Army radio. Israeli Defense Minister Shaul Mofaz made the announcement after meeting U.S. Secretary of Defense Donald Rumsfeld in Washington on November 4, with the Israeli Air Force looking to buy 100 of the new stealth jets, also known as the F−35. The aircraft, being developed by U.S. manufacturer Lockheed Martin and various other international partners, is due to come into service within 10 years. The agreement came after Mofaz promised that Israel would "respect its undertakings" to Washington concerning sales of sensitive military technology.
Source: http://www.defensenews.com/story.php?F=1226962&C=mideast

[Return to top]

Banking and Finance Sector

7. *November 08, Reuters* — **Scammers move online to beat UK chip and PIN system.** In the UK, credit card scammers are moving online because the introduction of "chip and PIN" card verification systems has made it harder commit fraud in person, the country's banking payment association said on Tuesday, November 8. The spread of chip and PIN −− which requires people to type in their card numbers when making purchases −− helped lead to a 13 percent fall in credit card fraud in the first six months of 2005, the first significant fall for 10 years, the Association for Payment Clearing Services (APACS) said. In contrast, Internet, telephone and mail order fraud −− collectively known as "card not present" crimes −− went up by 29 percent to over US$157 million with online fraud accounting for 64 percent of this. "The majority of this type of fraud is card details being stolen in the real world and then used to buy goods on the Internet," said APACS spokesperson Mark Bowerman. APACS, the trade association for organizations that deliver payment services to end customers, said 117 million of the country's 140 million payment cards have been upgraded to chip and PIN since the program began in late 2003.
APACS: http://www.apacs.org.uk/
Source: http://today.reuters.co.uk/news/NewsArticle.aspx?type=internetNews&storyID=2005−11−08T012410Z_01_SCH804905_RTRIDST_0_OUKIN−UK−BRITAIN−FINANCIAL−FRAUD.XML

8. *November 08, Arizona Daily Star* — **Indictments made in global theft ring.** Seventeen Tucson, AZ−area residents were indicted on charges of using stolen credit and debit card numbers and other personal information to steal money from ATMs as part of an international computer−based theft ring. The group used card numbers and other financial information supplied by people in foreign countries to make counterfeit bank or credit cards and then wired back half the stolen money as payment, officials said in announcing the federal indictments unsealed Monday, November 7. The Tucson residents had more than 4,500 illegally obtained credit and debit card numbers and personal−identification numbers, said Michael Moskaitis, an agent and spokesperson for the U.S. Secret Service. The suspects were also in possession of other personal information, such as Social Security numbers, addresses, passwords and other data needed to make the fake cards, Moskaitis said. The Tucson residents were recruited using Internet chat rooms by people in 19 countries such as Australia, Serbia and Montenegro, Mexico, Canada and Russia, said Harriet Bernick, spokesperson for the U.S. Attorney's Office in Arizona.
Source: http://www.azstarnet.com/metro/101465.php

9. *November 08, Portland Tribune (OR)* — **Possible identity thefts uncovered during drug raid.** Portland, OR, police are warning people to check their credit records and bank accounts after recovering during a drug raid a computer with personal information that could be used to steal the identities of hundreds of thousands of people. The information included mailing lists that once were sold legally by the Oregon Department of Motor Vehicles and credit information, including information from credit bureaus, that probably was obtained illegally. Details include hundreds of thousands of names, birth dates, home addresses, Social Security numbers and credit scores. According to Sgt. Mike Krantz of the East Precinct Crime Reduction Unit, the computer contained enough personal information to generate hundreds of thousands of false driver’s licenses and other forms of identification, many of which could be used to open charge accounts in the names of real people. Law enforcement agencies frequently find evidence of identity theft during methamphetamine investigations. In the past, both the

Portland police and the Multnomah County sheriff's office have displayed equipment used to produce methamphetamine and false identifications seized at the same raids.
Source: http://www.portlandtribune.com/archview.cgi?id=32555

[Return to top]

Transportation and Border Security Sector

10. *November 08, Associated Press* — **Airline faces fine after man gets on flight without ticket.** A New Jersey man boarded a plane in Newark, NJ, without having a ticket or boarding pass. Fort Worth−based American Airlines says federal airport screeners should have kept 29−year−old Danis Ballard off the flight. The man from Irvington, NJ, made it on to the plane on Saturday, November 5, but was removed before it took off for Miami. Authorities say Ballard used a worthless, printed flight itinerary to board. He's been charged with criminal trespass. American could be fined up to $25,000 for allowing Ballard to board.
Source: http://www.kristv.com/Global/story.asp?S=4090062

11. *November 08, Associated Press* — **Experts say cruises vulnerable, but lines defend security plans.** Just like a scene in a Hollywood blockbuster: Pirates fire rocket−propelled grenades and machine guns at a luxury cruise ship full of tourists off a lawless African country. The cruise crew tries to ram both pirate boats, uses an earsplitting high−tech weapon on the attackers, and evades them. That was the real−life situation the crew and passengers of the Seabourn Spirit found themselves in off Somalia last weekend. With piracy common in some areas and terrorism fears present after the September 11, 2001, attacks, cruise lines say they train their crews and have security measures to respond effectively to these threats. But security experts say that despite all the preparations, cruise liners are vulnerable to attacks like this one or the deadly bombing by al Qaeda−linked militants of the USS Cole in Yemen five years ago. Nonetheless, cruise industry officials said the Spirit's successful efforts to repel the attackers validate security plans that all ships must have in place under U.S. and international law. Cruise lines are in constant communication with authorities on land and the U.S. military responded to the attack on the Spirit, he said. The U.S. counterterrorism task force for the Horn of Africa is based in Djibouti, which borders Somalia.
Source: http://www.centredaily.com/mld/centredaily/business/13112856 .htm

12. *November 08, Associated Press* — **Texas border counties to increase manpower.** Counties along the border will have an additional dozen officers patrolling during every eight−hour shift as part of an initiative by Texas Border Sheriff's Coalition, chose Monday, November 7, to split a $6 million state grant −− part of a border protection package ordered by Governor Rick Perry −− evenly among its 16 member counties. Each county will each receive about $367,000 that will allow them to pay for equipment and the overtime of deputies, adding an extra layer of security along the state's border with Mexico, said the group's interim director, Rick Glancy. The increased manpower is part of "Operation Linebacker," a plan to add deputies and equipment in the state's 16 counties bordering Mexico. The plan was modeled after an El Paso County operation last year that led to more drug arrests and helped curb crime, said Glancy. Coalition members hope lawmakers in Washington will allow local law enforcement along the border to receive untapped Homeland Security funds, said El Paso County Sheriff Leo Samaniego, the group's vice chairman. The coalition formed in the spring to bring attention to

the homeland security and border violence concerns of local law enforcement.
Source: http://www.team4news.com/Global/story.asp?S=4089355&nav=0w0v

13. *November 07, Department of Transportation* — **Department of Transportation to tighten oversight of Amtrak.** Department of Transportation Secretary Norman Y. Mineta on Monday, November 7, announced the Department would implement recommendations to strengthen its oversight of Amtrak in light of a new Government Accountability Office (GAO) report that found widespread managerial problems within the company. Secretary Mineta, who said he agreed with the GAO's findings, also called on Amtrak to take quick steps to address the recommendations made in the November 3rd GAO report that require Board or management action. Mineta directed the Department's Federal Railroad Administration (FRA) to require Amtrak to submit its plans to improve financial reporting and management practices. The agency will monitor progress on the plans and issue a new annual report to Congress on how well Amtrak is improving its financial practices, Mineta added. The Secretary said Amtrak also would be required to demonstrate how it will improve its acquisition practices before receiving federal taxpayer grants. The FRA will award grants to Amtrak once it demonstrates that it has reformed its acquisitions practices. Mineta said, "The problems outlined in the GAO report demand attention and require that we finally make the tough choices needed to save Amtrak and improve intercity passenger rail service in this country."
Source: http://www.dot.gov/affairs/dot16305.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *November 08, Iowa Ag Connection* — **Corn is piling up outside in Iowa.** Hurricanes Katrina and Rita had a major impact on the corn industry in Iowa. Because river barge traffic was slowed down, it became more difficult to transport that crop. This season, corn has really been piling up in an unusual amount. From the minute each kernel pops out of the truck to the moment they spit into open air, a corn capped mountain is growing into a temporary storage site. Iowa corn stored outside has been building up this season, even doubling last year's crop −− all because it just won't fit inside. Four hundred thousand bushels have piled up outside in Manchester, IA. Each day, at least 20 trucks take what farmers harvest and deliver it to the pile.
Source: http://www.usagnet.com/story−national.cfm?Id=1122&yr=2005

15. *November 08, Stop Soybean Rust News* — **More soybean rust found in North Carolina.** Edgecombe County has become the northern−most county with soybean rust in both North Carolina and the U.S. The county is about five counties inland from the Outer Banks, and only three counties south of the Virginia border. North Carolina officials reported Edgecombe as positive Tuesday, November 8. With this find, the North Carolina total grows to 14 rust counties, and the U.S. now has 121.

Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=623

16. *November 07, South Dakota Department of Game, Fish and Parks* — **Two deer have tested positive in South Dakota's 2005 Chronic Wasting Disease Surveillance Program.** The South Dakota Department of Game, Fish and Parks (GFP) has been testing deer and elk from hunters, vehicle kills, and sick animals encountered in the field. Currently, 595 results have returned from the 820 total samples submitted, with two deer testing positive for chronic wasting disease (CWD). "The two deer that tested positive were both collected by GFP personnel that are on the watch for sick deer and elk," said GFP Wildlife Biologist Steve Griffin. "Both of these deer were found very emaciated and thin, which are symptoms of CWD. As in past years, GFP is conducting a CWD surveillance program in areas where CWD has been detected in captive animals, and/or in wild free−roaming populations of deer and elk. Surveillance is being concentrated in the southwestern part of South Dakota.
Source: http://www.sdgfp.info/GFPnews/News05/11−07−05.htm

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

17. *November 08, Reuters* — **Bird flu kills Vietnamese man.** Bird flu has killed a Vietnamese man, the country's 42nd victim, and is suspected in the death of another the government said on Tuesday, November 8. A 35−year−old man from Hanoi who died on October 29 after eating a chicken with his family was confirmed as the first human victim of the latest outbreak, said Nguyen Van Binh, deputy director of the Health Ministry's Preventive Medicine Department. The latest death comes as the European Union (EU) pledged funds to help Asia fight bird flu. On the second of a two−day visit to Hanoi, EU Commissioner for Health and Consumer Protection Markos Kyprianou said allocations would be decided by a meeting under way in Switzerland. The 35−year−old Vietnamese man developed a slight fever after eating the chicken and was taken to Bach Mai hospital on October 26 with respiratory difficulties. He died three days later. Doctors said they suspected bird flu also killed a 68−year−old man in the central province of Quang Tri on Sunday, November 6, a day after he was taken to the General Hospital in Hue city. The man had a critical lung infection and fever, among the clinical symptoms of bird flu infection.
Source: http://today.reuters.com/News/newsArticle.aspx?type=healthNews&storyID=2005−11−08T111427Z_01_RID840191_RTRUKOC_0_US−BIRDFLU−VIETNAM.xml

18. *November 08, Associated Press* — **U.S. urges United Nations group plan for bird flu.** The U.S. on Tuesday, November 8, proposed that the United Nations health agency immediately convene a small expert group to plan a rapid response in the event of a flu pandemic. The panel should also draft a plan to close gaps in influenza surveillance and complete both in time for consideration by the World Health Organization's (WHO) executive board in January, said Stewart Simonson, assistant secretary of the U.S. Health and Human Services Department. "We must go beyond generalized planning and well−intentioned expressions of cooperation," Simonson told a group of scientists and other experts meeting at WHO's Geneva, Switzerland, headquarters. Experts agree an eventual global flu pandemic capable of killing millions of people is a certainty. Scientists say it is also certain that the virus will come from bird flu. The U.S. believes the international community must take immediate steps to increase surveillance, particularly in Asia, Africa and Latin America, and agree on what actions must be taken and by whom when a pandemic strain emerges, Simonson said.
Source: http://www.miami.com/mld/miamiherald/living/health/13111888. htm

19. *November 08, PLoS Medicine* — **A malaria vaccine that elicits in humans antibodies able to kill Plasmodium falciparum.** Plasmodium falciparum merozoite surface protein 3 is a malaria vaccine candidate that was identified, characterised, and developed based on a unique immuno−clinical approach. The vaccine construct was derived from regions fully conserved among various strains and containing B cell epitopes targeted by human antibodies (from malaria−immune adults) that are able to mediate a monocyte−dependent parasite killing effect. The corresponding long synthetic peptide was administered to 36 volunteers, with either alum or Montanide ISA720 as adjuvant. Both formulations induced cellular and humoral immune responses. With alum, the responses lasted up to 12 months. This is the first malaria vaccine clinical trial to clearly demonstrate antiparasitic activity by vaccine−induced antibodies by both in vitro and in vivo methods. The results, showing the induction of long−lasting antibodies directed to a fully conserved polypeptide, also challenge current concepts about malaria vaccines, such as unavoidable polymorphism, low antigenicity, and poor induction of immune memory.
Source: http://medicine.plosjournals.org/perlserv/?request=get−document&doi=10.1371/journal.pmed.0020344

20. *November 08, Agence France Presse* — **Hong Kong stages first−ever bird flu drill.** Hong Kong hospital staff staged their first−ever bird flu drill as part of preparations to ward off possible outbreaks from neighboring countries. More than 70 frontline hospital staff at the Tuen Mun Hospital in the suburban New Territories took part in the exercise along with four other major hospitals in the territory. Simulating a response to the discovery of a policeman struck with the H5N1 virus, hospital staff were seen rushing into action, in teleconference calls with officials at the Hospital Authority's central command and coordinating with officials in other hospitals. Chief executive Donald Tsang and Health Secretary York Chow visited the hospital afterwards, saying the drill went very smoothly. The government said it will stage a larger−scale bird flu drill later this month involving more health workers.
Source: http://channels.netscape.com/news/story.jsp?id=2005110808057000000001&dt=20051108080500&w=AFP&coview=

21.

November 07, Agence France Presse — **Angola announces end of Marburg fever outbreak.** Angola is officially free of Marburg fever after an outbreak of the disease that killed 227 of the 252 people it infected over the last year, Health Minister Sebastao Veloso said. "There have been no cases of fever since July 27," he said. He revised downwards the toll taken by the outbreak. On September 19, he and the World Health Organization (WHO) said the epidemic had killed 329 people of 374 confirmed cases of infection. The latest Angolan outbreak began in October 2004 in a hospital in Uige province but was not formally identified until March 2005, by which time the epidemic had prompted the deployment of dozens of experts from the WHO and other organizations. There is no cure for the Marburg virus, whose exact origin is unknown and which was first detected in 1967 when West German laboratory workers in the town of Marburg were infected by monkeys from Uganda.
Marburg fever information: http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/marburg.htm
Source: http://news.yahoo.com/s/afp/20051107/hl_afp/angolahealthviruses_051107204917;_ylt=AkxP0OXt5ZIWv6VypFaUcBaJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

22. *November 07, Bloomberg School of Public Health* — **Scientists find evolutionary trade−off in spread of dengue fever.** Some viruses' ability to exploit the human body's own defenses to increase their replication may be both a blessing and curse, according to the findings of a study conducted by researchers at the Johns Hopkins Bloomberg School of Public Health. Scientists believe antibody−dependent enhancement may allow the dengue virus to grow more rapidly in people who were previously infected and have partial but incomplete immunity to the virus. Enhanced virus replication triggers a more deadly, hemorrhagic form of the disease. A study suggests that antibody−dependent enhancement offers an evolutionary trade−off between advantage and disadvantage for the dengue virus. The findings could one day lead to new strategies for developing and deploying vaccines. Using computational models based on epidemic theory, the researchers examined the dynamic role antibody−dependent enhancement plays in the spread of dengue viruses. They concluded that when antibody−dependent enhancement triggered small increases in transmission, it gave viruses an edge over other cocirculating dengue viruses that did not experience enhancement. Although the computer models were specifically developed for dengue, the researchers believe the results could apply to any disease in which partial immunity increases pathogen replication rates.
Dengue information: http://www.cdc.gov/ncidod/dvbid/dengue/index.htm
Source: http://www.jhu.edu/~gazette/2005/07nov05/07dengue.html

23. *November 07, University of Colorado* — **New "flu chip" may help combat future epidemics, pandemics.** A novel "flu chip" developed at the University of Colorado (CU) at Boulder that can determine the genetic signatures of specific influenza strains may help world health officials combat coming epidemics and pandemics. Tests on the technology by the U.S. Centers for Disease Control and Prevention (CDC) showed the CU−Boulder chip can determine the genetic make−up of types and subtypes of the flu virus in about 11 hours, said CU−Boulder Professor Kathy Rowlen. Current methods for characterizing flu subtypes infecting patients take about four days. Rowlen said they are conferring with CU's Technology Transfer Office and plan to make the Flu Chip genetic sequences freely available to interested researchers. There currently are less than 200 facilities worldwide that provide detailed strain analysis of influenza, said Rowlen. Strain identification is critical for tracking emerging strains and in

determining which flu strains are most likely to infect people the following year in order to develop annual, preventative vaccines, she said. The chip, which can be configured to test for all known flu virus strains as well as new variant strains, was evaluated for three primary subtypes of flu in the October CDC test. The chip was more than 90 percent accurate. Source: http://www.colorado.edu/news/releases/2005/424.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24. *November 08, Associated Press* — **District of Columbia government would run city shelters in disaster situations.** Under a plan being worked out by District of Columbia officials, the city's Department of Human Services would replace the American Red Cross in spearheading local mass emergency care operations if a natural disaster or act of terrorism were to strike. The changes are being suggested following the city's experience with 274 Hurricane Katrina evacuees, who were housed in the DC Armory and were not able to find temporary or permanent housing for nearly a month. Barbara Childs−Pair, director of the District's Emergency Management Agency, said, "Many of the resources that we thought Red Cross would have on hand, we ended up having to go out and procure right away." The city's disaster response plan is being changed to list the Red Cross as a support agency. Childs−Pair says the city has purchased 444 hospital beds to supplement the number of beds available at the Washington area's 11 major hospitals. Over the past four years, the city has spent about $8 million to improve hospital readiness under a bioterrorism preparedness program funded by the U.S. Department of Defense. During a drill held last week, the hospitals relayed requests for transportation, medical supplies, and equipment through the city's emergency operations center. Source: http://www.wtopnews.com/index.php?nid=251&sid=615544

25. *November 08, Government Accountability Office* — **GAO−06−246T: Hurricanes Katrina and Rita: Preliminary Observations on Contracting for Response and Recovery Efforts (Testimony).** The devastation experienced by those throughout the Gulf Coast in Louisiana, Mississippi, Alabama, and Texas in the wake of Hurricanes Katrina and Rita has called into question the government's ability to effectively respond to such disasters. The government needs to understand what went right and what went wrong, and to apply these lessons to strengthen its disaster response and recovery operations. The federal government relies on partnerships across the public and private sectors to achieve critical results in preparing for and responding to natural disasters, with an increasing reliance on contractors to carry out specific aspects of its missions. At the same time, the acquisition functions at several agencies are on the Government Accountability Office's (GAO) high−risk list, indicating a vulnerability to fraud, waste, abuse, and mismanagement. GAO was asked to provide an overview of (1) its role in evaluating the contracting community with regard to disaster preparedness and response, (2) GAO's plans for reviewing the performance of the federal government and its contractors in

preparing for and responding to the hurricanes, and (3) what GAO has learned so far about the performance of the federal government and its contractors in preparing for and responding to the hurricanes.
GAO Highlights: http://www.gao.gov/highlights/d06246thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−246T

26. *November 07, Portland Press Herald (ME)* — **Maine asks towns to identify disaster leaders.** To firm up emergency action plans, Maine officials are encouraging all communities to adopt local ordinances detailing who will be in charge at different stages of an emergency and to create an inventory of responders. Having the plan will help to ensure that the towns and state will qualify for federal grants for disaster preparedness. Arthur Cleaves, director of the Maine Emergency Management Agency, said, "All our incidents happen at a local level. Somebody at the local level will be in charge of that incident…Understanding that chain of command and who is in charge is essential in any emergency." The initiative comes at the request of the federal government's National Incident Management Program, which requires identifying the resources available within a community and making sure department managers know the expectations for their departments. Starting in 2007, homeland security funding will be available only to communities that have codified a chain of command and met training requirements. Cleaves also commented on the importance of training all levels of government in disaster preparedness: "We want to be sure to reach all of the public officials beyond the first responders, who have not been trained at that level or in that detail."
Source: http://pressherald.mainetoday.com/news/local/051107respond.s html

[Return to top]

Information Technology and Telecommunications Sector

27. *November 08, US−CERT* — **Technical Cyber Security Alert TA05−312A: Microsoft Windows Image Processing Vulnerabilities.** Microsoft has released updates that address critical vulnerabilities in Windows graphics rendering services. A remote, unauthenticated attacker exploiting these vulnerabilities could execute arbitrary code or cause a denial of service on an affected system. The Microsoft Security Bulletin for November 2005 addresses multiple buffer overflows in Windows image processing routines. Viewing a specially crafted image from an application that uses a vulnerable routine may trigger these vulnerabilities. If this application can access images from remote sources, such as Websites or e−mail, then remote exploitation is possible. Microsoft has provided the updates to correct these vulnerabilities in Microsoft Security Bulletin MS05−053.
MS05−053: http://www.microsoft.com/technet/security/bulletin/MS05−053. mspx
Source: http://www.us−cert.gov/cas/techalerts/TA05−312A.html

28. *November 07, FrSIRT* — **MagpieRSS "httpsrequest" function remote command execution issue.** A vulnerability has been identified in MagpieRSS, which could be exploited by remote attackers to execute arbitrary commands. The vulnerability is due to an input validation error in the " httpsrequest" function of Snoopy when passing malformed URLs to the "exec()" call, which could be exploited by remote attackers to execute arbitrary commands via a specially crafted URL. FrSIRT recommends upgrading to MagpieRSS version 0.72.
Source: http://www.frsirt.com/english/advisories/2005/2335

29. *November 07, Boston.com* — **Federal Communications Commission says no cutoff for Internet phone customers.** According to guidance from the Federal Communications Commission (FCC) released on Monday, November 7, Internet telephone providers will not have to cut off service to U.S. subscribers even if they are not able to receive enhanced 911 (E911) emergency service. Internet telephone providers had worried that the FCC's rules adopted in May would required them to suspend by November 28 service for subscribers who cannot receive E911 service. According to the recently released guidance, existing customers do not have to be disconnected, but Internet telephone providers will have to cease marketing and accepting new customers in areas where they are not connecting 911 calls with the person's location and phone number. The voice−over−Internet−protocol (VOIP) rules adopted in May required 911 calls to be routed to live dispatchers and the caller's location and number be identified. The move followed instances in which customers had trouble reaching help when they dialed 911. The Voice On the Net Coalition, which represents many VOIP providers, said that roughly 750,000 customers could be affected if they had to suspend service to those who did not have enhanced 911 service available.
FCC guidance: http://www.fcc.gov/headlines.html
Source: http://www.boston.com/business/technology/articles/2005/11/08/us_fcc_says_no_cutoff_for_internet_phone_customers/

30. *November 06, SecuriTeam* — **Cisco IOS heap−based overflow vulnerability.** The Cisco Internetwork Operating System (IOS) may permit arbitrary code execution after exploitation of a heap−based buffer overflow vulnerability. In many cases, a heap−based overflow in Cisco IOS will simply corrupt system memory and trigger a system reload when detected by the "Check Heaps" process, which monitors for such memory corruption. In a successful attack against an appropriate heap−based overflow, it is possible to achieve code execution without the device crashing immediately. Successful exploitations of heap−based buffer overflow vulnerabilities in Cisco IOS software often result in a Denial of Service. In some cases it is possible to overwrite areas of system memory and execute arbitrary code from those locations. In the event of successful remote code execution, device integrity will have been completely compromised. Cisco has included additional integrity checks in its software that are intended to reduce the likelihood of arbitrary code execution. The advisory is posted on Cisco's website.
Cisco: http://www.cisco.com/en/US/products/products_security_advisory09186a008055ef31.shtml
Source: http://www.securiteam.com/securitynews/6E0011PEKA.html

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 publicly available proof of concept code for an Oracle worm. Currently, US−CERT cannot confirm if this code works. We are working with Oracle to determine the threat posed by this

code.

Although there is limited information concerning this potential threat, US−CERT strongly encourages Oracle system administrators to implement the following workarounds:

* Change default user credentials for Oracle installations

* Change the default port for the TNS listener

* Restrict Oracle network access to trusted hosts only

* Revoke CREATE DATABASE LINK privileges from the CONNECT role

US−CERT will continue to investigate the issue and provide updates as they become available.

For more information please review URL:
http://www.us−cert.gov/current/current_activity.htmloraclewm

Malicious Website / Malicious Code: XML−RPC for PHP Worm

US−CERT is currently aware of a new worm which targets web servers running vulnerable versions of XML−RPC for PHP. Once the worm infects a web server, it opens a backdoor to the compromised server and begins scanning for additional servers to infect. Versions of XML−RPC for PHP prior to 1.1.1 are vulnerable. XML−RPC for PHP is used in many third party products, including:

* AWStats

* PHPGroupWare

* phpMyFAQ

* PHPWik

* TikiWiki

For more information please review URL:
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =331

Current Port Attacks

Top 10 Target Ports	35885 (−−−), 1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 6346 (gnutella−svc), 80 (www), 135 (epmap), 25 (smtp), 40000 (−−−), 1025 (win−rpc) 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

31. *November 07, Associated Press* — **A school scare in Maryland.** Arrowhead Elementary School in Upper Marlboro, MD, was locked down on Monday morning, November 7, when a man with a gun was seen in the area. Police say an officer on routine patrol noticed a man dressed in a black mask and a black jacket and armed with a long gun. When the officer approached the man, he ran toward the school and tried to get in through the rear door. The door was locked, and the man ran off. Police searched the area with tactical teams, but had not found the man by Monday night. No shots were fired.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=44250

[Return to top]

General Sector

32. *November 08, Associated Press* — **Australians say raids foiled terror attack.** Police arrested 17 terror suspects in Australia's two biggest cities Tuesday, November 8, in raids authorities said foiled a plot to carry out a catastrophic terror attack. A radical Muslim cleric known for praising Osama bin Laden was charged with masterminding the plot. More than 500 police backed up by helicopters were involved in raids across Sydney and Melbourne, arresting eight men in Sydney and nine in Melbourne and seizing chemicals, weapons, computers, and backpacks. Nine men appeared Tuesday, November 8, in Melbourne Magistrates Court charged with being members of a terror group. Prosecutor Richard Maidment told the court the nine planned to kill "innocent men and women in Australia. The members of the Sydney group have been gathering chemicals of a kind that were used in the London Underground bombings." He said they underwent military−style training at a rural camp northeast of Melbourne. Seven men arrested in Sydney were held in cells at a downtown court during a five−minute hearing Tuesday, November 8, at which they were ordered held until another hearing on Friday, November 11, on charges of preparing a terror act by manufacturing explosives.
Source: http://abcnews.go.com/International/wireStory?id=1291400

[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