Department of Homeland Security Daily Open Source Infrastructure Report for 10 November 2005

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

Daily Highlights

- The Washington Post reports Social Security numbers and other information about more than 3,000 consumers housed on a desktop computer was stolen recently from TransUnion LLC, one of three U.S. companies that maintain credit histories on individuals. (See item 4)
- International health experts have agreed on the outlines of a global strategy to tackle the spread of bird flu that the World Bank has estimated would cost up to $1 billion over three years, with a comprehensive strategy to address all aspects from veterinary services to providing access to anti−viral drugs. (See item 22)
- The DHS Daily Open Source Infrastructure Report will not be published on Friday, November 11, due to the observance of a federal holiday. The next issue will be on Monday, November 14.

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 09, Nbc6.net (FL)* — **Thousands still without power in Florida.** Florida Power & Light says it has restored power to more than three million customers who lost power when Hurricane Wilma hit South Florida on October 24. In Miami−Dade County, 16,000 customers

are still without power, 32,500 have no power in Broward County and 400 customers are without electricity in Palm Beach County. The utility hopes to have the restoration of power complete by midnight Friday, November 11.
Outage numbers by county: http://www.fpl.com/storm/contents/wilma_outage.shtml
Source: http://www.nbc6.net/news/5287098/detail.html?rss=ami&psp=new s

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *November 08, KRON 4 (CA)* — **Shell refinery releases chemical cloud, prompting issuance of health advisory.** Contra Costa County, CA, Health Services says a chemical cloud that leaked from the Shell Refinery has mostly dissipated. But, they have issued a health advisory for the area surrounding the plant. The leak was reported around 8:30 p.m. PST Tuesday, November 8, in one of the plant's processor units. It released a chemical cloud that rose up into the air but officials say it did not drift outside of the plant's site.
Source: http://www.kron4.com/Global/story.asp?S=4093187&nav=5D7i

3. *November 07, Associated Press* — **U.S. Chemical Safety and Hazard Board investigates deaths at Delaware refinery.** The U.S. Chemical Safety and Hazard Board (CSB) sent two investigators Monday, November 7, to assess whether the deaths of two workers at a Delaware refinery merits a comprehensive probe. The men died Sunday, November 6, when they entered a nitrogen gas−filled silo at Valero Energy's refinery in Delaware City, DE, and succumbed to fumes. Valero, based in San Antonio, TX, said the men were contract workers authorized to work in the area, but neither was authorized to enter the silo.
Source: http://www.greenwichtime.com/business/investing/sns−ap−refinery−deaths,0,662765.story?coll=sns−ap−investing−headlines

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

4. *November 09, Washington Post* — **Data on thousands of consumers stolen with computer.** Social Security numbers and other information about more than 3,000 consumers were stolen recently from TransUnion LLC, one of three U.S. companies that maintain credit histories on individuals. The data was housed in a desktop computer that was stolen last month from a regional sales office in California, TransUnion said. On October 21, the company sent 3,623 notices to consumers alerting them to the breach and offering free monitoring of their credit reports for a year. Colleen Tunney, vice president of corporate affairs for Chicago−based TransUnion, said the computer was probably the object of the burglary, not the data. She said the information on the computer required a password to access. Tunney said the company is

investigating why such information would be stored on an individual computer in a regional office rather than on a secure corporate network.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/11/08/AR2005110801573.html

5. *November 09, Government Technology* — **New report surveys and analyzes technologies to combat phishing.** The Anti−Phishing Working Group and SRI International on Tuesday, November 8, announced the availability of a new report mapping the spectrum of current and future technology solutions to combat Internet fraud, or phishing schemes. The report, "Online Identity Theft: Technology, Chokepoints and Countermeasures," was commissioned by the Department of Homeland Security Science and Technology Directorate. Intended for technical practitioners, researchers and security executives, the report offers a comprehensive survey and analysis of counter−phishing technology. The report details technologies used by online identity thieves and explores technologies that could dramatically reduce financial losses and consumer distrust.
Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures: http://www.antiphishing.org/Phishing−dhs−report.pdf
Source: http://www.govtech.net/magazine/channel_story.php/97221

6. *November 08, Reuters* — **Bank customers do less online banking according to survey.** Even as banks and regulators increase efforts to thwart identity theft over the Internet, the worry that scammers remain one step ahead is convincing many Americans that banking online is too risky. At an identity theft forum in New York on Tuesday, November 8, security and policy experts said banks are taking appropriate steps to stop online criminals, but that their best efforts −− and consumers' own vigilance −− may not be enough. An October survey commissioned by Internet security company Entrust Inc. and released at the forum found that 18 percent of Americans who have banked online now do so less, or not at all, because of security concerns. Ninety−four percent say they're willing to accept extra online security protections.
Survey information: http://www.entrust.com/news/2005/6126_6342.htm
Source: http://today.reuters.co.uk/news/NewsArticle.aspx?type=internetNews&storyID=2005−11−08T203422Z_01_HAR874019_RTRIDST_0_OUKIN−UK−FINANCIAL−BANKS−IDTHEFT.XML

[Return to top]

Transportation and Border Security Sector

7. *November 09, Christian Science Monitor* — **High tech sniffers to stop “dirty” bombs.** If a terrorist tried to sneak a "dirty" bomb into the United States, radiation detectors rushed into service since 9/11 might sound the alarm at seaports, border checkpoints, and mail−handling facilities. Then again, the sensors have been set off by everything from loads of kitty litter to bananas. Also, a smart terrorist could hide a basketball−size chunk of highly enriched uranium by using lead shielding less than an inch thick. That's why the U.S. is set to begin deploying a new generation of radiation detectors intended to be America's "last line of defense" against weapons of mass destruction. By early spring, the Department of Homeland Security will pick technologies from among 10 companies, whose newest generation of nuclear detectors was

tested in the Nevada desert this summer. Their devices will begin field−testing at a few ports of entry by next June, with a full−production decision expected by 2007. That pace may be picking up as disturbing evidence accumulates. About a year ago, the National Intelligence Council warned that "undetected smuggling has occurred, and we are concerned about the total amount of [nuclear and radiological] material that could have been diverted or stolen in the past 13 years" around the world.
Source: http://www.csmonitor.com/2005/1109/p01s03−ussc.html

8. *November 08, Department of Homeland Security* — **Department of Homeland Security provides Visa Waiver Program report to Congress.** The Department of Homeland Security (DHS) on Tuesday, November 8, announced the completion of a status report on countries participating in the Visa Waiver Program (VWP) as required by the Enhanced Border Security and Visa Entry Reform Act of 2002. As a result of this review, 25 of the 27 participating countries will maintain their current enrollment status in the Visa Waiver Program. Comprehensive reviews of Italy and Portugal are on a different time schedule and the results of those reviews will be released at a later time. Information included in the report covers sensitive information relating to terrorism, criminal activities, illegal immigration, and alien smuggling, and therefore is classified in accordance with appropriate executive orders. The country reviews are only one requirement for participation in the VWP. Recently announced requirements for VWP countries regarding digital photos passports and e−passports are separate from this country review process. The 27 countries participating in the VWP are Andorra, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom.
Source: http://www.dhs.gov/dhspublic/display?content=4928

[Return to top]

Postal and Shipping Sector

9. *November 08, Government Computer News* — **Postal Service to act as PIV I service center under pilot plan.** The U.S. Postal Service (USPS) will use its experience in facilitating passport applications to help agencies meet the requirements for Homeland Security Presidential Directive−12. Under a pilot program, USPS will provide the Office of Personnel Management (OPM) with identity proofing services that comply with Personal Identity Verification I (PIV I) under an interagency agreement. The Postal Service is acting as a service provider, where OPM will pay about $30 per employee. OPM will use as many as 10 USPS facilities around the country to provide these services in major cities such as Atlanta and Boston, said Lolie Kull, co−chair of the working group. Kull gave a presentation about the working group on Tuesday, November 8, at a Government Smart Card Interagency Advisory Board meeting in Washington, DC.
Homeland Security Presidential Directive−12:
http://www.whitehouse.gov/news/releases/2004/08/20040827−8.h tml
Source: http://www.gcn.com/vol1_no1/daily−updates/37530−1.html

10. *November 08, Government Computer News* — **USPS may require Parcel Select clients to use e−voucher system.** The U.S. Postal Service is weighing whether to require all customers of its

Parcel Select program to use an electronic system that the agency hopes will help ease payment and verification for mail acceptance. In a proposed rule, the Postal Service also said its Electronic Verification System (e−VS) may be expanded for all users if it demonstrates cost savings and efficiencies during its initial rollout. E−VS is an electronic manifest program for tracking payments and verifying all Parcel Select mailings, and it is expected to replace an inefficient and complex paper filing database. Parcel Select is a ground delivery program for medium−to−large customers. Under e−VS, mailers will bar code all packages and submit an electronic manifest to the Postal Service. The manifest contains data such as weight, destination and induction facility to support postage and fee information.
Rule: http://a257.g.akamaitech.net/7/257/2422/01jan20051800/edocket.access.gpo.gov/2005/05−22156.htm
Source: http://www.gcn.com/vol1_no1/daily−updates/37528−1.html

[Return to top]

Agriculture Sector

11. *November 09, Wisconsin Ag Connection* — **Man sentenced to prison for freeing mink.** An animal rights activists who plead guilty to domestic terrorism charges for freeing thousands of mink from Midwest fur farms will go to federal prison for two years. Peter Young of Mercer Island, WA, was sentenced on Tuesday, November 8, by U.S. District Judge Stephen Crocker. He was also ordered to pay nearly $255,000 in restitution to the farmers he violated. Young eluded authorities for more than seven years after he trespassed on the mink operations eight years ago. Young, and accomplice Justin Samuel set out to cripple the fur industry in 1997 −− freeing more than 7,000 mink from their cages at five farms in Iowa, South Dakota, and Wisconsin. The two were indicted in 1998 on four counts of interference with commerce by threat or violence and two counts of animal enterprise terrorism. Authorities in 1999 picked up Samuel, who agreed to cooperate in exchange for a two−year prison sentence. Young was a fugitive until March when he was arrested on a shoplifting charge.
Source: http://www.wisconsinagconnection.com/story−state.cfm?Id=1339 &yr=2005

12. *November 09, Agricultural Research Service* — **DNA chips spot, help track antibiotic resistance.** A genetic chip that detects more than 100 antimicrobial−resistance genes in bacteria has been developed by Agricultural Research Service (ARS) scientists in Georgia. The DNA chip, called a DNA microarray, is a small glass slide that allows researchers to determine the presence or absence of particular DNA sequences in a sample. ARS microbiologists developed the DNA microarray to detect genes that make bacteria resistant to antibiotics. Antimicrobial compounds, or antibiotics, have been used for years to fight bacterial infections. But some bacterial pathogens, like Salmonella and Campylobacter, and other intestinal bacteria, like Escherichia coli and Enterococcus, are becoming resistant to antibiotics. Unfortunately, under the right conditions, DNA that's linked to resistance may be exchanged between bacteria when they come together. Scientists need to know which bacteria are resistant to antibiotics and how bacteria continue to develop resistance to new antibiotics. The researchers use the microarrays to track resistant genes in bacteria from farm and slaughter facility samples. This information will help identify possible points to target for intervention strategies to prevent the development and spread of resistance.
Source: http://www.ars.usda.gov/is/pr/2005/051109.htm

13. *November 09, Animal and Plant Health Inspection Service* — **Grant program for national animal identification.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) Wednesday, November 9, announced it will award three million dollars in cooperative agreements to states and tribes for conducting research to develop or test potential solutions for animal identification and automated data collection in support of the National Animal Identification System (NAIS). Applicants are encouraged to propose research or field trial projects enhance the effectiveness of collecting animal identification data in typical production, market and abattoir environments; establish identity validation when official identification devices are lost, removed or malfunction; conduct economic assessments of animal identification systems and technologies in typical production, market and abattoir environments; and evaluate emerging animal identification technologies with advanced data collection systems to ascertain the adaptability of the technology for use in NAIS. Projects applicable to any livestock or animal industry associated with NAIS are eligible for funding. Collaboration with private companies, producer organizations, colleges and universities, or other research organization is strongly encouraged. Implementation of NAIS will support state and federal animal disease monitoring and surveillance through the rapid tracing of infected and exposed animals during animal disease outbreaks.
Source: http://www.aphis.usda.gov/lpa/news/2005/11/NAISTRIAL.html

[Return to top]

Food Sector

14. *November 08, Queen's University (Canada)* — **New protein discovery may have implications for treating deadly E. coli infection.** In a study funded by the Canadian Institutes for Health Research, Queen's University researchers may have identified a more effective treatment of a deadly strain of the E. coli bacteria with the discovery of a previously unknown protein. A team led by biochemistry researcher Zongchao Jia identified a protein that allows the bacterial strain known as E. coli 0157:H7 to obtain the iron it needs for survival. The newly discovered protein breaks down heme, releasing the iron atom stored there for use by the deadly bacteria. According to Jia, "This discovery opens the door for studying the function of heme iron in this strain of E. coli, and may lead to an understanding of how to therapeutically isolate the protein to keep the bacteria from thriving."
Study: http://www.pnas.org.
Source: http://qnc.queensu.ca/story_loader.php?id=4370a99fa9139

15. *November 08, Food Safety and Inspection Service* — **Chicken product recalled.** Garden Leaf Foods, a Gardena, CA, firm, is voluntarily recalling approximately 275 pounds of a ready−to−eat chicken product that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday, November 8. The deli wraps were distributed to retail stores in Arizona, California, Nevada, and New Mexico. The problem was discovered through FSIS microbiological sampling. FSIS has received no reports of illnesses associated with consumption of the products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_048_2005_relea se/index.asp

16. *October 11, Government Accountability Office* — **GAO−06−157R: Mad Cow Disease: An Evaluation of a Small Feed Testing Program FDA Implemented in 2003 With Recommendations for Making the Program a Better Oversight Tool (Correspondence).** In 1997, the Food and Drug Administration (FDA) banned the use of most proteins derived from mammals (referred to as prohibited material) in feed intended for cattle and other ruminants. The feed−ban rule is one of the primary actions taken by the federal government to protect U.S. cattle from bovine spongiform encephalopathy (BSE), commonly known as mad cow disease, which is believed to be spread through feed that contains malformed protein found in certain tissue of BSE−infected animals. The feed testing program is a small part of FDA's BSE oversight effort and is one of several methods FDA uses to monitor for compliance with the feed−ban rule. However, several weaknesses in the design and implementation of the feed testing program need to be addressed to improve its effectiveness. Specifically, under the program guidance, FDA did not require districts to document their follow−up reviews or the basis for their final determinations on samples that the laboratories identified as potentially containing banned protein products. For nearly half the 989 samples, FDA took longer than 30 days from the date the sample was collected until the date the laboratory completed its analysis. By the time FDA conducted its follow up to determine whether a violation had occurred, the feed may have been consumed.
Source: http://www.gao.gov/new.items/d06157r.pdf

[Return to top]

Water Sector

17. *November 09, Metro West Daily News (MA)* — **Boston suburb's water tests positive for E. coli.** Water samples taken from two locations in Holliston, MA, Wednesday, November 2, tested positive for the E. coli bacteria Tuesday, November 8. Testing on samples taken Friday, November 4, and Monday, November 7, showed no E. coli, otherwise known as fecal coliform bacteria, but continued to indicate the presence of total coliform bacteria at various locations. The Massachusetts Department of Environmental Protection issued a mandatory water boil order Wednesday, November 8, after the test results came back.
Massachusetts Department of Environmental Protection: http://www.mass.gov/dep/
Source: http://www.metrowestdailynews.com/localRegional/view.bg?arti cleid=113842

18. *November 08, Philadelphia Business Journal (PA)* — **Aqua America buys water systems.** Subsidiaries of Aqua America have bought four water systems. The Bryn Mawr, PA, company, which provides water and wastewater services, bought systems in North Carolina, Illinois, and Pennsylvania. The company's purchases are in addition to its acquisition of 24 water and wastewater systems through the first three quarters of the year. Aqua America is the largest U.S.−based publicly traded water utility, serving more than 2.5 million residents in the Carolinas, Pennsylvania, Ohio, Illinois, Texas, Florida, New Jersey, Indiana, Virginia, Maine, Missouri, and New York.
Source: http://philadelphia.bizjournals.com/philadelphia/stories/200 5/11/07/daily19.html

[Return to top]

Public Health Sector

19. *November 09, Medical News Today* — **British Airways mislaid bird flu sample from Romania for a few days.** A sample of suspected bird flu from Romania went missing at Heathrow airport, London, and could not be found for one or perhaps two days. British Airways transported the sample from Romania. However, as a security team came to pick it up they could not find it. According to the airline no one was at risk at any time. British Airways says it is carrying out an investigation.
Source: http://www.medicalnewstoday.com/healthnews.php?newsid=33287#

20. *November 09, Associated Press* — **Vietnam to produce generic bird−flu drug.** Vietnam has reached an agreement with the manufacturer of the antiviral drug Tamiflu to allow the country to produce a generic version starting early next year in an effort to protect its population against bird flu, according to Nguyen Van Thanh, deputy director of the pharmaceutical administration department under the Health Ministry. Tamiflu is one of the few medications believed to be effective in treating bird flu. Roche Holding AG developed oseltamivir, known by the trademarked name Tamiflu, but cannot keep up with soaring demand. According to Thanh, Roche will provide the materials and technical assistance to Vietnam so it can produce oseltamivir. The company has also agreed to supply Vietnam with 25 million Tamiflu capsules, enough to treat 2.5 million people. According to a Health Ministry statement, the first batch of two million pills will be available in December, and the rest will be provided by August 2006. Several other countries, including India and China, have been in talks with Roche about licenses to produce Tamiflu.
Source: http://health.yahoo.com/news/_126361

21. *November 09, Agence France−Press* — **Eritrea to begin nationwide child polio vaccination campaign.** According to the World Health Organization (WHO), Eritrea will this week launch a nationwide polio vaccination campaign to immunize children under five as part of an Africa−wide operation aimed at halting the spread of the virus. The inoculation campaign comes two months after one polio case was detected near the border with Sudan and several other cases reported in Yemen, Sudan and Ethiopia. WHO representative Andrew Kosia said, "We have detected one case but it does not mean there is only one case. It can spread very fast…Eritrea is at risk because there have been cases in neighboring countries. In Yemen, across the Red Sea, there have been 450 cases. In Sudan, over 100 cases, and in Ethiopia, some 30 cases." Health workers will go from house to house across the country to inoculate children under five between November 11 and 14 and again from December 16.
Source: http://news.yahoo.com/s/afp/20051109/hl_afp/healtheritreapolio_051109114255&printer=1;_ylt=AopGtvE1nI30s7rbovnYOuqKOrgF;_ylu=X3oDMTA3MXN1bHE0BHNlYwN0bWE−

22. *November 09, Reuters* — **World health experts outline bird flu strategy.** On Wednesday, November 9, international health experts agreed on the outlines of a global strategy to tackle the spread of bird flu that the World Bank has estimated would cost up to $1 billion over three years. Wrapping up three days of talks, World Health Organization (WHO) Director−General Lee Jong−Wook said the strategy covered minimizing the virus threat at source in animals and humans, strengthening early warning systems, strengthening veterinary services, improving countries' pandemic preparedness, making access to anti−viral drugs fairer, and supporting

more research into pandemic vaccines. According to Jong−Wook, "This meeting had identified a series of integrated actions that will start straight away." He highlighted improved communication to the public as a priority and said a donor mechanism should be put in place. The World Bank has proposed a financing framework, which it said would be focused on funding "country−owned programs" to combat the spread of the H5N1 virus. The World Bank has said its package would contain both grants or interest−free loans for countries, while half of the $1 billion needed will be funded by a trust financed by donors.
Director−General's remarks: http://www.who.int/dg/lee/speeches/2005/closingremarks_avianflu/en/index.html
Source: http://www.alertnet.org/thenews/newsdesk/L09735508.htm

23. *November 08, University of Rochester Medical Center* — **Grants to fund research on preparing for bioterrorist attack.** Research teams at the University of Rochester Medical Center in New York have received two $10 million grants from the National Institute of Allergy and Infectious Diseases to help ready the nation to defend itself against terrorist attacks where viruses or bacteria are used as weapons. One grant will establish the Center for Biodefense Immune Modeling, which will develop mathematical models and computer simulations of how the human immune system responds to influenza A and smallpox. Such simulations could help researchers devise countermeasures, including new ways to boost the body's ability to fight disease. According to Hulin Wu, Ph.D., professor and division chief, Department of Biostatistics and Computational Biology, "The infection simulator would allow us to think like would−be bioterrorists, testing in cyberspace how the body responds to viruses that have been engineered to be even deadlier…Should bioweapons never be used, the work better prepares us for a future attack by nature itself, perhaps in the form of a bird flu pandemic." The second grant will establish the Program for Biodefense of Immunocompromised Populations, whose goal will be to find ways to help those most vulnerable to bioterrorist attack to survive despite having weaker immune systems.
Source: http://www.eurekalert.org/pub_releases/2005−11/uorm−gt110805 .php

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24. *November 09, Daily Times Chronicle (MA)* — **Massachusetts fire captain praises outcome of mock disaster.** Reading, MA, firefighters joined with firefighters from several area cities and towns as they participated in a successful mock disaster at the Anderson Regional Transportation Center on Sunday morning, November 6, that pitted a passenger train versus a tanker. According to Woburn Fire Captain Robert Mills, who participated in the early morning exercise, the mock disaster certainly proved to be a valuable learning experience for local emergency responders. In addition to Woburn safety officials, Burlington, Reading, Winchester and Massachusetts Bay Transportation Authority (MBTA) officers, among other community

firefighters, partook in the full−scale emergency response exercise, which lasted approximately four hours. According to Mills, the exercise was extremely valuable in preparing regional communities for a large−scale disaster that involves coordination and cooperation amongst multiple local and state agencies, especially when it comes to understanding the chain−of−command during such incidents. According to MBTA officials, the purpose of the exercise was to ensure an efficient and professional operational response to the emergency situation.
Source: http://www.woburnonline.com/frontpage/november05/11705−3.htm l

25. *November 08, Oak Ridger (TN)* — **Regional emergency response forum held in Tennessee.** Hundreds of emergency response personnel, officials with Department of Energy (DOE), and representatives of sponsors UT−Battelle and the Tennessee Emergency Management Agency participated in the fifth annual Oak Ridge Regional Emergency Forum held in Oak Ridge, TN, on Thursday, October 27. The annual forum, themed "Practical Applications in Emergency Response Saves Lives," was the fifth in a series held in an effort to work toward building relationships between various agencies and to bring together government, law enforcement and first responders along with other entities in an effort to share ideas, experiences and technology in the field of emergency response. "There is much that can be learned by bringing together various first−responder agencies. We all walked away from this forum more informed and better able to effectively deal with emergencies that we might experience at our site offices," said Robert Brown, chief operating officer of the DOE's Oak Ridge Office. Lessons learned about emergency management responses were shared with the forum participants. The event showcased vendor and agency exhibits on display, hands−on testing of equipment, emergency response vehicles and various other cutting edge technology used for emergency response.
Source: http://www.oakridger.com/stories/110805/new_20051108036.shtm l

26. *November 08, Courier−Journal (KY)* — **Computer glitch turns 911 calls into headache for dispatchers.** A glitch in Louisville, KY's, MetroSafe emergency dispatch system clogged all 32 of the city's 911 lines for about two hours Monday night, November 7, and forced dispatchers to call back everyone who might have been missed while the lines were jammed, said Chad Carlton, a spokesperson for Louisville Metro Mayor Jerry Abramson. Earlier in the day, the MetroSafe computer−aided dispatch system got a routine software upgrade. By about 9 p.m. EST, dispatchers were unable to disconnect a 911 call when it was completed. All 32 of the city's lines at the Barret Avenue dispatch center quickly filled up, leaving new callers to 911 unable to get through. The city's emergency management team worked with BellSouth, its telecommunications provider, to reroute the lines, Carlton said. The city's enhanced 911 system is supposed to show dispatchers the telephone numbers and addresses of callers. By 11 p.m. EST, the 911 system could take calls again, though dispatchers did not have the specific address of the callers readily available.
Source: http://www.courier−journal.com/apps/pbcs.dll/article?AID=/20051108/NEWS01/511080412/1008/NEWS01

27. *November 08, Associated Press* — **Air Force general: Hurricane Katrina provided lessons for terrorism.** The military learned lessons from Hurricane Katrina that can be applied to future disasters ranging from a major terrorist strike to an avian flu pandemic, an Air Force general says. Katrina in many ways mirrored the kind of mass casualty emergency that would result from a chemical, biological, radiological or nuclear attack, Major General M. Scott Mays

said Monday, November 7. "It's hard to say that anything good came out of Katrina, but I have to tell you it was a dress rehearsal to an event of that magnitude" for the military, Mays said. Mays is commander of the 1st Air Force. Headquartered at nearby Tyndall, FL, Air Force Base, his command is responsible for the air defense of the contiguous 48 states. Consisting mainly of National Guard units scattered across the U.S., the 1st Air Force is part of the U.S. Northern Command, which is conducting a terrorism exercise this week called, "Vigilant Shield '06." It is a large command post exercise that includes responding to a mock radiological bomb detonated by terrorists and a simulated nuclear missile attack on Washington, DC.
Source: http://www.tallahassee.com/mld/tallahassee/13112801.htm

28. *November 08, Washington Post* — **Thousands of Hurricane Katrina 911 calls went astray.** Early in the afternoon of August 29, as Hurricane Katrina bore down on the Gulf Coast, the phones inside the Louisiana State Police emergency operations center began ringing with frantic pleas for help. However, floodwaters had forced 120 operators at the 911 center to abandon the New Orleans police headquarters. Emergency calls were supposed to be routed to the fire department but its main station was already abandoned. And so many calls were shunted north to Baton Rouge, LA. The disintegration of New Orleans's 911 system carries national implications for future disasters, said public safety experts. While some communities boast sophisticated, high−tech centers with elaborate contingency plans, most cities have older systems lacking adequate backup measures for massive disasters. "People in our country have gotten to believe that no matter what kind of trouble you get into, all you have to do is dial 911," said William Smith, chief technology officer at BellSouth, which is the phone carrier for New Orleans 911 calls. "That's not necessarily the case." The 911 network is actually little more than a patchwork, subject to the budgetary pressures and technological whims of local and state governments, with no national standards.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/11/07/AR2005110701334.html

[Return to top]

Information Technology and Telecommunications Sector

29. *November 09, FrSIRT* — **VERITAS NetBackup volume manager daemon buffer overflow issue.** A vulnerability has been identified in VERITAS NetBackup, which could be exploited by remote attackers to execute arbitrary commands or cause a denial of service. This is due to a buffer overflow error in a shared library used by the volume manager daemon (vmd) that does not properly handle specially crafted requests port 13701, which could be exploited by remote attackers to execute arbitrary commands with root/SYSTEM privileges. FrSIRT reports that this issue is formally resolved in NetBackup Enterprise Server/Server Security Packs.
Security Packs: http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNLOAD.htm
Source: http://www.frsirt.com/english/advisories/2005/2349

30. *November 08, Security Focus* — **Microsoft Windows graphics rendering engine WMF/EMF format code execution vulnerability.** Multiple vulnerabilities were identified in Microsoft Windows, which could be exploited by remote attackers to execute arbitrary commands or cause a denial of service. The first issue is due to heap overflow errors in "GDI32.DLL" when

processing malformed Windows Metafile (WMF) and Enhanced Metafile (EMF) images, which could be exploited by convincing a user to visit a malicious Website using Internet Explorer, read a malicious email using Outlook, or open a specially crafted Office document containing a malicious image. The second flaw is due to an integer overflow error in the "PlayMetaFileRecord()" function of "GDI32.DLL" that does not properly handle malformed Windows Metafile (WMF) images, which could be exploited by convincing a user to visit a malicious Website using Internet Explorer, read a malicious email using Outlook, or open a specially crafted Office document containing a malicious image. The third vulnerability is due to an error in the "GetEnhMetaFilePaletteEntries()" function of "GDI32.DLL" when processing malformed Enhanced Metafile (EMF) images, which could be exploited to cause a denial of service via a malicious image. Security Focus reports that Microsoft has released a bulletin that includes fixes for supported versions of the operating system.
Bulletin: http://www.microsoft.com/technet/security/bulletin/ms05−nov. mspx
Source: http://www.securityfocus.com/bid/15352/references

31. *November 08, FrSIRT* — **VERITAS cluster server for UNIX local buffer overflow vulnerability.** A vulnerability has been identified in VERITAS Cluster Server for UNIX, which could be exploited by local attackers to execute arbitrary commands or cause a denial of service. This flaw is due to a buffer overflow error when handling calls to multiple "ha" commands associated with the VCSI18N_LANG environment variable, which could be exploited to execute arbitrary commands with root privileges. FrSIRT reports that there are security fixes available.
Security Fixes: http://seer.support.veritas.com/docs/279870.htm
Source: http://www.frsirt.com/english/advisories/2005/2350

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:
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:
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

32. *November 09, Brown Daily Herald (RI)* — **Surveillance cameras on campus triple.** Surveillance cameras on the Brown University campus have tripled in number in the past five years. The cameras −− many of them housed in black, hemispherical shells −− are sprinkled around campus. The increase at Brown is typical of higher education institutions −− one security consultant said cameras are currently the number one security item for colleges and universities. In recent years, as the technology of camera systems has improved and prices have dropped, institutions have widely increased camera usage, according to several security professionals. In a 2003 article, the Chronicle of Higher Education reported that Brown's campus had 60 cameras in 2000 and 105 in 2003. That number is 180 today, with slightly more cameras outdoors than indoors, according to David Cardoza, technical and support systems manager. Cardoza said the cameras are in high−traffic areas and "places where we've had past instances of crime or we've had problems in the past."
Source: http://media.www.browndailyherald.com/media/paper472/news/2005/11/09/CampusNews/Surveillance.Cameras.On.Campus.Triple−1050823.shtml?sourcedomain=www.browndailyherald.com&MIIHost=me

dia.collegepublisher.com

33. *November 09, Government Accountability Office* — **GAO−06−244T: Army Corps of Engineers: History of the Lake Pontchartrain and Vicinity Hurricane Protection Project (Testimony).** The greatest natural threat posed to the New Orleans area is from hurricane−induced storm surges, waves, and rainfalls. A hurricane surge that can inundate coastal lowlands is the most destructive characteristic of hurricanes and accounts for most of the lives lost from hurricanes. Hurricane surge heights along the Gulf and Atlantic coasts can exceed 20 feet. The effects of hurricane Katrina flooded a large part of New Orleans and breeched the levees that are part of the U.S. Army Corps of Engineers (Corps) Lake Pontchartrain, and Vicinity, Louisiana Hurricane Protection Project. This project, first authorized in 1965, was designed to protect the lowlands in the Lake Pontchartrain tidal basin from flooding by hurricane−induced sea surges and rainfall. The Government Accountability Office (GAO) is providing information on (1) the purpose and history of the Lake Pontchartrain, and Vicinity, Louisiana Hurricane Protection Project and (2) funding of the project. GAO is not making any recommendations in this testimony.
Highlights: http://www.gao.gov/highlights/d06244thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−244T

[Return to top]

General Sector

34. *November 09, Reuters* — **Three suspected suicide bombers hit three hotels in Jordan.** Three suspected suicide bombers blew themselves up at three international hotels in Jordan's capital on Wednesday, November 9, killing and wounding many people, the official Jordanian news agency said. Reuters correspondents said there had been explosions at Radisson SAS and Grand Hyatt hotels in Amman and the official Petra news agency said there had been a third blast at the Days Inn hotel in the city. The agency said the blasts had been caused by suspected suicide bombers and there were many dead. Police threw up roadblocks around the hotels, causing traffic chaos in the city, and Reuters television footage showed a fleet of ambulances and fire vehicles outside the buildings. The blasts appeared to happen at much the same time. A Reuters correspondent at the Radisson said five people were killed there and more than 12 others wounded. Another correspondent at the Hyatt hotel said at least 40 were wounded, some seriously, there. Witnesses said many Western tourists were staying at the three hotels.
Source: http://ca.today.reuters.com/news/NewsArticle.aspx?type=topNews&storyID=2005−11−09T204222Z_01_SPI968949_RTRIDST_0_NEWS−SECURITY−JORDAN−COL.XML

[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