Department of Homeland Security Daily Open Source Infrastructure Report for 31 October 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports the Anti−Spyware Coalition has published guidelines to help consumers assess products designed to combat unwanted programs that sneak onto computers. (See item 5)
- The Detroit Free Press reports a federal grand jury in Detroit has indicted 25 people in one of the largest drug and money laundering conspiracies in Michigan. (See item 8)
- The Transportation Security Administration is making thousands of screeners nationwide complete five hours of training to detect bombs hidden in carry−on luggage or under a traveler's clothing. (See item 10)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *October 29, The Seattle Times* — **Leads sought in substation theft.** The theft recently of more than $7,000 worth of electrical equipment from Bonneville Power Administration's (BPA) Covington Substation in Kent, WA, was added to the decade−old BPA's Crime Witness Hotline program, which offers up to $25,000 for information leading to the arrest and conviction of those responsible for crimes. The agency has some 350 substations in a six−state area in the

Northwest, and though many are fenced, many also are unattended during evenings and weekends, said Pete Jeter, the BPA's lead physical−security specialist. He said thieves go for cabling, wires and other electrical components that are high in such materials as copper and aluminum, selling them to recyclers. He said that for the past two years, between one and three substations a month have been broken into.
Source: http://seattletimes.nwsource.com/html/localnews/2002590703_dige29m.html?syndication=rss

2. *October 28, Associated Press* — **Man accused of sabotaging Arizona gas lines.** A fired employee of a natural gas distribution company has been indicted on charges he sabotaged the utility's pipelines by puncturing them and tampering with valves, authorities said. A federal indictment released Friday, October 28, charges Thomas Lee Young, 58, with 16 counts of destruction of energy facilities between November 2000 and December 2002, and two counts of mailing threatening communications. Young is accused of sabotaging Southwest Gas Corp. facilities in Pima and Pinal counties in southern Arizona. The company said there were 30 acts in all −− including puncturing of plastic lines with screws or drills and the manipulation of valves to under− or over−pressurize parts of the system. Three customer outages were recorded by Southwest Gas, but there were no fires, explosions, ruptures or injuries. The company estimated the sabotage cost it more than $500,000.
Source: http://news.yahoo.com/s/ap/20051029/ap_on_re_us/pipeline_sabotage_1

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *October 28, Porterville Recorder (CA)* — **Workers evacuate winery due to exposure of unknown chemical.** Thirty−seven people −− including a one−year−old child −− exposed to a unknown chemical at a Richgrove, CA, winery Thursday morning, October 27, scrambled to several local hospitals with complaints of eye, throat and chest irritation. Officials at Sierra View District Hospital, where 16 people drove themselves for treatment, shut down the emergency room for three hours after what they said may be the largest contamination incident in recent memory. But officials at the Castle Rock Winery said there were no detectable levels of hazardous gases Thursday morning. Patients were treated for possible sulfur dioxide exposure and released Thursday afternoon. However, because the patients' symptoms were relatively mild, doctors were unable to confirm the actual presence of sulfur dioxide.
Source: http://www.portervillerecorder.com/articles/2005/10/28/news/local_state/news01.txt

4. *October 27, Cullman Times (AL)* — **Explosives truck spills chemicals, causing business evacuation and road closure.** Businesses along a half−mile section of Alabama Highway 157−South in Cullman, AL, were evacuated and the road was closed to through traffic for eight hours Wednesday, October 26, as city, county and state officials oversaw the containment and cleanup of a chemical spill from an explosives truck. The spill itself involved no explosive material, but rather consisted of an oxidizing gel which when combined with ammonium nitrate and diesel fuel creates an explosive material often used in demolition. What concerned local officials was the fact that all three ingredients (oxidizing agent, ammonium nitrate, diesel fuel) were being transported on this one vehicle. Around 8:30 a.m. EDT Wednesday Police Sgt. Jeff Warnke was conducting routine traffic patrol north along Childhaven Road when he noticed the

Austin Powder Co. truck traveling north bound on 157 leaking what smelled like diesel fuel. Warnke estimated that the fluid spilled for a distance of close to a half−mile, from Childhaven Road to just south of the U.S. Highway 31 and Highway 157 intersection, by the time he got the truck stopped. The cleanup was completed and the highway reopened around 4:30 p.m. EDT.
Source: http://www.cullmantimes.com/story.php?id=2354

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *October 31, Associated Press* — **Anti−spyware group publishes guidelines.** A coalition of anti−spyware vendors and consumer groups published guidelines Thursday, October 27, to help consumers assess products designed to combat unwanted programs that sneak onto computers. The Anti−Spyware Coalition released the guidelines for public comment and also updated a separate document that attempted to craft uniform definitions for spyware and adware in hopes of giving computer users more control over their machines. According to the Pew Internet and American Life Project, Internet users have become more cautious online because of worries about spyware and adware, which can bombard users with pop−up ads and drain processing power to the point of rendering computers unusable. The new guidelines from the coalition assign risk levels to various practices common with spyware and adware. High−risk practices include installation without a user's permission or knowledge, interference with competing programs, interception of e−mail and instant−messaging conversations and the display of ads without identifying the program that generated them. A separate coalition document defining spyware and related terms changed little from the draft issued in July.
Final Working Report of the Spyware Definitions and Supporting Documents:
http://www.antispywarecoalition.org/documents/definitions.ht m
Anti−Spyware Coalition Risk Model Description:
http://www.antispywarecoalition.org/documents/riskmodel.htm
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/10/27/AR2005102700819.html

6. *October 28, Knoxville News Sentinel (TN)* — **Personal information about university students exposed.** Earlier this month a University of Tennessee (UT) student put her name into the Google search engine and discovered her name and Social Security number posted on a UT e−mail discussion group site. It turns out the nine−month−old listserv's archives had inadvertently been made public, exposing the personal information of nearly 2,000 current and former UT students and a handful of faculty and other users, UT officials said Thursday, October 27. Officials said they have no indication any of the data has been accessed or used by unauthorized individuals. The listserv, a term referring to one of the original computer programs that allowed distribution of e−mail messages among specified groups, was made up of about 10 individuals and a small number of departments including UT's Bursar's Office and

the Office of Information Technology's application development department, said Brice Bible, UT interim chief information officer. The listserv was set up to exchange information regarding small financial transactions such as payment of library fines and laboratory fees that are not taken care of under the school's automated payment systems, Bible said. Apparently in setting up the program, a parameter was set that allowed archives of the discussion to be public, Bible said, although participation in the discussion remained internal.
Source: http://www.knoxnews.com/kns/business/article/0,1406,KNS_376_4193016,00.html

7. *October 28, Australia Associated Press* — **Online banking scheme disrupted.** West Australian police say they have cracked an illegal Internet banking syndicate. They have arrested and charged a 24−year−old computer engineer with more than 30 offenses, including 15 counts of stealing and 15 of unlawful access of a computer. More charges are expected to be laid with other suspected members of the syndicate likely to be charged later, said Detective Constable Duncan Taylor. He said police had been tracking a gang for the past three months. Multiple banks and financial institutions had been targeted, he said, but declined to name them. Dozens of customers had become unwitting victims and a significant amount of money had been stolen by the gang, he said. Gang members gained Internet banking customers' private information, including names and passwords, using keylogging computer programs and then fraudulently transferred cash from their accounts, he said.
Source: http://australianit.news.com.au/articles/0,7204,17063105%5e15306%5e%5enbv%5e,00.html?from=rss

8. *October 28, Detroit Free Press* — **Federal grand jury indicts twenty−five in drug, money laundering scheme.** A federal grand jury in Detroit has indicted 25 people in one of the largest drug and money laundering conspiracies in Michigan. The gang, known as the Black Mafia Family, distributed more than 1,000 pounds of cocaine in metro Detroit and laundered more than $270 million in drug proceeds since the early 1990s, officials said. The alleged ringleaders, Terry and Demetrius Flenory of Detroit, moved drugs and money nationwide in cars with hidden compartments. One of the more novel methods the gang used to launder drug proceeds was to buy more than $1 million worth of winning lottery tickets from Michigan residents and redeem the tickets to buy houses and cars, authorities said. The gang operated in California, Georgia, Kentucky and Missouri. The indictment named 23 other people who allegedly managed or helped distribute drugs and cash or launder drug proceeds.
Source: http://www.freep.com/news/latestnews/pm6991_20051028.htm

9. *October 28, Agence France−Presse* — **U.S. links North Korean counterfeit currency to weapons of mass destruction.** A U.S. official warned that North Korea's mass production and distribution of counterfeit U.S. currency is likely funding the proliferation of weapons of mass destruction. Stuart Levey, the U.S. Treasury's undersecretary for terrorism and financial intelligence, said the U.S. government was extremely concerned about Pyongyang's production of large amounts of high−quality fake U.S. bills. "You have to come to the conclusion that the counterfeit is supporting the proliferation," he said. Levey said the high−quality counterfeits, also known as Supernotes, were eventually laundered to fund illicit activities of the Communist regime. "There are a variety of ways that counterfeit currency can be put into legitimate financial system and ultimately laundered so it produces value for the government of North Korea," he said. "It's something that we take extraordinarily seriously," he said, declining to put a value to the fake notes that have been distributed.

Source: http://news.yahoo.com/s/afp/20051028/pl_afp/usnkoreachinawea pons_051028142554

[Return to top]

Transportation and Border Security Sector

10. *October 28, Associated Press* — **Newark airport screeners to increase preparedness on bomb detection.** Security screeners at New Jersey's Newark Liberty International Airport are among those who soon must undergo additional training to help detect bombs hidden in carry−on luggage or under a traveler's clothing. The Transportation Security Administration is making thousands of screeners nationwide complete five hours of training by Tuesday, November 15. Security experts remain concerned about a terrorist smuggling an explosive onto a plane because X−ray machines and metal detectors don't detect such materials. To compound the problem, heavy passenger loads and the agency's goal of holding down wait times at security checkpoints have complicated the effort to detect explosives. Authorities have considered a variety of other technologies to look for bombs, including a machine that provides an X−ray image of a passenger's body. A machine, known as a "puff portal," has been installed in some airports. Passengers enter a booth and short bursts of air hit their bodies, dislodging particles that are then examined by a computer for bomb residue. Newark has two of them, one in Terminals A and B, and three others are planned for Terminal C. But even then, only a small number of passengers can be tested by the machines.
Source: http://www.newsday.com/news/local/wire/newjersey/ny−bc−nj−−airportscreeners−1028oct28,0,725647.story?coll=ny−region−apne wjersey

11. *October 28, Marin Independent Journal (CA)* — **San Francisco bridge has anti−terror campaign.** Golden Gate Bridge officials are hoping to enlist the public's help in thwarting potential terrorist activities. Posters have gone up on district ferries, buses, and the bridge itself as part of its public awareness program. The brightly colored placards show an abandoned backpack with an arrow pointing it out. The placards read "See Something? Say Something!" and instructs people to "report suspicious ... packages, people, and activities," and provides contact information for reporting something out of the norm. About 400 posters are being distributed throughout the district's transportation facilities, including aboard buses and ferries, at bus and ferry transit terminals, and at various locations at the bridge. The U.S. Coast Guard has been randomly boarding Golden Gate ferries and providing occasional escorts for the vessels as part of increased security in the wake of terrorist bombings. Additionally, a Coast Guard−sponsored security program is already in place, using local law enforcement agents on the boats. Marin County sheriff's deputies along with Sausalito, Twin Cities and San Francisco police have agreed to ride along randomly. The program began in September 2004.
Source: http://www.marinij.com/marin/ci_3160296

12. *October 28, Reuters* — **Delta to merge Song with main fleet.** Delta Air Lines Inc. will close down its low−cost carrier Song, the bankrupt airline said on Friday, October 28, as it focuses on turning around its core operations. The decision, a victory for discount rival JetBlue Airways Corp. and a setback for Delta, whose previous management had hoped Song could compete against discount carriers like JetBlue. Delta, the number three U.S. carrier, said Song would stop operating as a separate unit in May 2006, about three years after it started flying. After May 2006, Song's narrow−body jets will be redeployed to other Delta routes −− mostly

transcontinental −− to replace wide−body planes the airline is shifting to international routes, Delta said.
Source: http://www.nytimes.com/reuters/business/business−airlines−de lta.html

13. *October 27, Associated Press* — **New border security program arrives in Northwest.** The Department of Homeland Security has expanded its program for electronically reading the faces and fingerprints of international visitors who try to enter the U.S. to seven border crossings in Eastern Washington and Idaho, the agency said Thursday, October 27. The United States Visitor and Immigrant Status Indicator Technology (US−VISIT) program uses optical and digital scanners to log and identify travelers who need a passport and visa to enter the U.S. The program has been used at the 50 busiest land border ports of entry −− including Blaine, WA −− since December 29, 2004, and was also in place at 115 airports and 15 seaports. Last week it became operational at remote border crossings in the Northwest. Those ports of entry are Porthill, ID, plus Danville, Laurier, Frontier, Boundary, Metaline Falls, and Ferry in Eastern Washington. US−VISIT will be in place at all 165 land border crossings by the end of the year.
Source: http://seattlepi.nwsource.com/local/6420AP_WA_Border_Securit y.html

14. *October 27, Canadian Press* — **Canadian military research technology group conducts marine security trial.** A Canadian−led marine surveillance experiment that involved tracking a metal cask from Liverpool, England, to it's intended drop off point in Nova Scotia's Chedabucto Bay as part of a maritime security exercise, is being called a success. Using a diverse array of satellite, sonar, radar, unmanned aerial surveillance and stealth buoys, researchers were able to track the mock contraband and eventually seize it as it was transferred between four vessels. "The object of the exercise was to collect data from different sensors on a common incursion scenario into the Maritimes," said navy Cmdr. Anthony Cond, project co−ordinator for the $3.5 million Maritime Sensor Integration Experiment. Cond said that in a post 9−11 world, knowing what's happening off Canada's coasts 24 hours a day is critical to marine security. An array of equipment was brought into play, including land, sea and air−sensing technology that allowed trackers to know where the barrel was virtually every second it was at sea. Researchers will now take the next several months to examine the data and try to refine the use of the technology. Much of what they find will be shared with other countries, such as the United States and Britain.
Source: http://cnews.canoe.ca/CNEWS/TechNews/TechInvestor/2005/10/27 /1281448−cp.html

15. *October 27, U.S. Department of State* — **International conference amends maritime treaties on unlawful acts.** New provisions that add significant counterterrorism, nonproliferation and ship boarding procedures to existing international agreements have been adopted by a diplomatic conference held by the International Maritime Organization (IMO) in London in October. The changes include a new protocol to the United Nation’s Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (SUA) and a companion amendment to Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf. The SUA protocol provides the first international treaty framework for combating and prosecuting anyone who uses a ship as a weapon or as a means to carry out a terrorist attack, or who transports terrorists or cargo destined to support weapons of mass destruction (WMD) programs by ship. The pact also establishes a mechanism to facilitate boarding of ships suspected of engaging in these activities in international waters. The new nonproliferation language strengthens the international legal

basis to impede and prosecute the trafficking of WMD and associated delivery systems and related materials on the high seas in commercial vessels by requiring state parties to criminalize such transport.
Additional information on Maritime Security provided by the IMO:
http://www.imo.org/Safety/mainframe.asp?topic_id=551
Full text of the IMO convention:
http://www.imo.org/Conventions/mainframe.asp?topic_id=259&do c_id=686
Additional information on the Proliferation Security Initiative and U.S. Policy:
http://usinfo.state.gov/is/international_security/arms_contr ol.html
Source: http://usinfo.state.gov/xarchives/display.html?p=washfile−english&y=2005&m=October&x=20051027150304sjhtrop0.5999109&t=livefeeds/wf−latest.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

16. *October 28, Agricultural Research Service* — **Rice researchers fight straighthead disease and improve grain quality.** Rice breeding lines that resist a costly disease, as well as lines with desirable grain characteristics, have been identified by Agricultural Research Service (ARS) scientists in Arkansas. Wengui Yan, a research geneticist at the ARS Dale Bumpers National Rice Research Center in Stuttgart, AR, leads efforts to analyze the U.S. Department of Agriculture (USDA) Rice Core Collection. With 1,791 entries, this genebank has been estimated to contain more than 70 percent of the genetic variation in the National Small Grains Collection's 18,408 rice accessions. Utilizing the core collection, Yan and his ARS colleagues identified germplasm accessions that are very resistant, or even immune, to straighthead, a plant disease that causes the entire rice head to remain upright at maturity with sterile florets and reduced grain yield. There is no straighthead resistance in commercial U.S. rice cultivars, but Yan has identified 26 indica and japonica rice lines that are resistant. Breeders at the University of Arkansas and Louisiana State University have incorporated some of these germplasm lines into their programs. Straighthead yield losses can reach almost 100 percent if a highly susceptible variety is planted in the wrong conditions.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

17. *October 27, U.S. Department of Agriculture* — **U.S. Department of Agriculture expands soybean rust risk management tool.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns announced Thursday, October 27, that USDA is again funding projects to track the spread of soybean rust and create the Pest Information Platform for Extension and Education to provide producers with information about additional legume pests and diseases. The nationally coordinated network will help producers in making crop management decisions that reduce pesticide input costs, reduce environmental exposure to pesticides and increase the efficiency

and efficacy of pesticide applications. The risk management tool component of the network is an online, real−time data system that allows growers and their advisors to access the latest information, to the county level, of where there are confirmed disease and/or pest outbreaks. The mapping tool will include frequently updated commentaries from state extension specialists and national specialists discussing immediate and projected risks and control options. To compliment the network, USDA will continue to conduct teleconferences, workshops and organize extension field visits to prepare first detectors to scout for pest and disease problems, to obtain diagnostic confirmation when a suspected problem is found and to manage the information for timely incorporation into the risk management map. Training modules will also be produced.
Soybean rust risk management tool: http://www.sbrusa.net
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2005/10/0465.xml

[Return to top]

Food Sector

18. *October 29, Agence France Presse* — **Japanese Foreign Minister says early resumption of U.S. beef imports likely.** Japanese Foreign Minister Nobutaka Machimura says Japan is likely to resume U.S. beef imports by the end of this year. Machimura, visiting Washington for the so−called "two−plus−two" talks of foreign and defense ministers, made the comments after meeting with U.S. Secretary of State Condoleezza Rice and White House National Security Adviser Stephen Hadley, Kyodo News said. While Machimura said he did not give any clear date during the talks, he told reporters before the meeting, "I have an expectation that we could make a decision by the end of the year to resume imports." The comment came after U.S. senators introduced legislation that would impose retaliatory tariffs over the Japanese ban on US beef imports. The bill, introduced by a bipartisan group of 20 senators, directs the U.S. administration to impose tariffs on Japanese exports to the United States if Tokyo does not lift its ban on beef by December 31.
Source: http://news.yahoo.com/s/afp/20051029/hl_afp/japanusbeefpolitics_051029065101;_ylt=AjcOQjEd3iUkdCKm7ctu9oyJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

19. *October 28, Associated Press* — **U.S. invests cash against bird flu.** The federal government said Thursday, October 27, it has awarded a $62−million contract to Chiron Corp. to manufacture a bird flu vaccine, and the Senate moved to invest far more −− eight billion dollars

−− on preparations in case the flu strain sparks a worldwide epidemic. The $62 million Chiron deal is the second contract for bird flu vaccine awarded by the government. Sanofi−Aventis has a $100−million contract to produce anti−bird flu shots. The Senate's out−of−budget expenditure would increase stockpiles of antiviral drug Tamiflu, antiviral Relenza, and vaccine, and boost emergency preparations at state and local levels.
Source: http://www.newsday.com/news/health/ny−bztami284486948oct28,0,7479100.story?coll=ny−health−headlines

20. *October 28, Associated Press* — **Texas probes 15 cases for dengue fever.** Health officials are investigating 15 cases in Brownsville, TX, for dengue fever, one of which they believe was contracted from a mosquito in the U.S. The U.S.−based case, a woman believed to be in her 20s or 30s, was diagnosed with dengue hemorrhagic fever. She received medical care and survived. Two other cases also have the more serious dengue hemorrhagic fever, while the others might have dengue fever, said Brian Smith, director of the Texas Department of State Health Services region that includes South Texas. Dengue hemorrhagic fever, which is more common in Asia, the Pacific, and Latin America, has been diagnosed in the U.S. in the past, but those people were bitten by mosquitoes in other countries, said Jim Schuermann, staff epidemiologist for the state health department. The two cases with dengue hemorrhagic fever were bitten by mosquitoes outside of the U.S., possibly in Mexico, Smith said. The Brownsville woman had dengue fever before and acquired the more serious illness June 26.
Dengue fever information: http://www.cdc.gov/ncidod/dvbid/dengue/index.htm
Source: http://news.yahoo.com/s/ap/20051028/ap_on_he_me/dengue_fever;_ylt=AkSNKvq2OpTLGq6W09Of0vBZ24cA;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

21. *October 27, Reuters* — **World Health Organization urges protective clothing for poultry workers.** Poultry workers, cullers, and veterinarians should wear special clothing and take antiviral drugs to protect them from bird flu, the World Health Organization (WHO) said on Thursday, October 27. All those at "high risk of exposure," working on farms with bird flu outbreaks or at risk of them, should wear coveralls, rubber gloves, surgical masks, goggles, and rubber boots, and could take an antiviral drug, it said. "These measures are particularly important during veterinary investigations and extensive and urgent culling operations," the WHO said. Humans suspected of having caught the lethal H5N1 strain of bird flu should be placed in immediate isolation, investigated, and checked for signs such as fever for 14 days, it added. The WHO also urged countries to share samples and viruses isolated from infected humans with its network of laboratories to permit quick analysis and guide national disease control strategies. The H5N1 strain has killed 62 people in four countries in Asia since re−emerging in 2003 and has recently been found among birds in Croatia, Romania, Turkey, and Russia, but no human cases have been reported in Europe.
Source: http://news.yahoo.com/s/nm/20051027/hl_nm/who_clothing_dc

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

22. *October 29, News−Register (OR)* — **Oregon county to stage mass inoculation exercise.** The United States isn't facing an influenza crisis this year, but Yamhill County, OR, health officials will still prepare for one. In a couple of weeks, all 556 Yamhill County employees will be run through a mandatory flu vaccination exercise. Shots won't be required, although they will be available free of charge to willing subjects. Officials worked out the details this week of a mass vaccination clinic set for November 9. The purpose is to simulate an emergency situation in which vaccinations are provided on a mass scale. "We're trying to jam a lot of people through in a short period of time," said Matt Jaqua, one of the county's public health officers. The exercise enables the county to comply with Federal Emergency Management Agency requirements. The county had planned a similar exercise in 2004, but it was called off when flu vaccinations were reported to be in short supply. Public safety and first responders routinely participate in emergency training exercises, but it's not often that such a drill involves all county staff. The last such event came in April 2003, when a drill was held to test the county's response to a 9.0 earthquake.
Source: http://www.newsregister.com/news/story.cfm?story_no=200111

23. *October 28, Post−Tribune (IN)* — **School district prepares for emergency.** Porter County, IN, first responders and administrators from the Porter Township school district dissected their disaster options Thursday, October 27. Termed a “tabletop exercise,” the training helps emergency personnel and school officials prepare for the unexpected. The training was provided through a $500,000 U.S. Department of Education grant, made available by the Northwest Indiana Educational Service Center in Highland. Its executive director, Charles Costa, said the grant is being used to train 113 schools in 18 school corporations throughout Lake and Porter counties. Christine Bredhold, a security consultant from New York, led Thursday’s session. She created a scenario for school and emergency workers in which a tanker truck filled with chlorine overturned near Boone Grove High School. A chemical plume was headed toward the school and would arrive in about an hour. “There isn’t enough time to get enough bus drivers to the school to evacuate 500 students,” Boone Grove High School principal said Garry DeRossett said. “It’s best we shelter in place and begin with a lock down.” During a lock down, no one gets in or out of the school. Because of the nature of the spill, the building would have to be sealed until it was out of danger.
Source: http://www.post−trib.com/cgi−bin/pto−story/news/z1/10−28−05_z1_news_12.html

24. *October 28, Fire Chief (IL)* — **DHS announces ninth round of firefighters grants.** The Department of Homeland Security (DHS) has announced the ninth round of the Fiscal Year 2005 Assistance to Firefighters Grant Program, awarding 540 grants to fire departments throughout the United States. This ninth round of fire grants provides $55,698,805 to help local fire departments and emergency medical services programs to purchase or receive training, first responder health and safety programs, equipment and response vehicles. AFGP will issue approximately 5,500 awards worth nearly $600 million in direct assistance to firefighters and first responders throughout the country, demonstrating Homeland Security's commitment to ensuring that America's firefighters have the resources they need to protect their communities. A complete list of recipients is available at http://www.firegrantsupport.com/afg/awards/05/
Source: http://firechief.com/news/fire_grants_9_10282005/

[Return to top]

Information Technology and Telecommunications Sector

25. *October 28, New York Times* — **Department of Justice approves two large telecom deals.** The Department of Justice (DOJ) has approved the sale of AT&T to SBC Communications and the sale of MCI to Verizon Communications, although the sale is still subject to approval by the Federal Communications Commission and several state regulators. Antitrust regulators at DOJ made few demands on SBC and Verizon despite protests from smaller phone companies that the deals would reduce competition. SBC and AT&T agreed to give rivals access to network buildings where both companies have facilities and where they are the only companies operating. Regulators made a similar request of Verizon and MCI. According to estimates by the Yankee Group, the acquisitions will allow SBC and Verizon to cumulatively control 56 percent of the $135 billion market. The next largest competitor will be Qwest Communications with seven percent, followed by BellSouth and Sprint, each with six percent.
Source: http://www.nytimes.com/2005/10/28/technology/28phone.html

26. *October 27, Security Focus* — **Apache Mod_Auth_Shadow authentication bypass vulnerability.** Apache Mod_Auth_Shadow is prone to a vulnerability that may bypass expected authentication routines. An attacker can exploit this vulnerability to bypass security restrictions and gain access to sensitive or privileged information. Information obtained may be used in further attacks against the underlying system. Security Focus reports that Debian Linux has released security advisory DSA−844−1 addressing this issue.
Security Advisory: http://www.securityfocus.com/bid/15224/solution
Source: http://www.securityfocus.com/bid/15224/discuss

27. *October 27, Security Focus* — **Novell ZENworks patch management multiple SQL injection vulnerabilities.** ZENworks Patch Management is prone to multiple SQL injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user supplied input before using it in SQL queries. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. These vulnerabilities can only be exploited if a non−privileged account has been created. Only an administrator can create such an account. Security Focus reports that Novell has addressed these issues in ZENworks Patch Management version 6.2 and later.
Novell Upgrade ZEN_PatchMgmt_Upd6.2.iso
http://download.novell.com/Download?buildid=5_kRStyf9wU~
Source: http://www.securityfocus.com/bid/15220/references

28. *October 27, Security Focus* — **Sun Solaris Management Console HTTP TRACE information disclosure vulnerability.** Sun Solaris Management Console is prone to an information disclosure vulnerability. The Solaris Management Console (smc(1M)) is a graphical user interface that provides access to Solaris system administration tools which includes a Web server that runs on port 898. The SMC Web server enables the HTTP TRACE method by default which may allow a local or remote unprivileged user the ability to access sensitive information −− such as cookies or authentication data −− contained in the HTTP

headers of an HTTP TRACE request. Security Focus reports that Sun has addressed these issues with a patch or workaround.
Patch: http://sunsolve.sun.com/search/document.do?assetkey=1−26−102 016−1
Source: http://www.securityfocus.com/bid/15222/references

29. *October 27, Security Focus* — **Kaspersky anti−virus Klif.Sys privilege escalation vulnerability.** Kaspersky Anti−Virus for Microsoft Windows 2000 platforms is prone to a privilege escalation vulnerability. The issue manifests in the Kaspersky kernel driver 'klif.sys', and may result in the execution of attacker−supplied code in the context of the system kernel (ring−0).
Exploit:/data/vulnerabilities/exploits/KAV_exploit.zip
Source: http://www.securityfocus.com/bid/13878/references

30. *October 27, TechWeb* — **Bird flu Trojan poses danger to Word users.** A new Trojan horse, dubbed "Navia.a" by Panda Software, uses subject heads of "Outbreak in North America" and "What is avian influenza (bird flu)?" to dupe recipients into opening an attached Microsoft Word document. Luis Corrons, director of Panda's research, says “Unfortunately, we were expecting something like this…This is not the first time, and won't be the last, that writers of malicious code have taken advantage of people's misfortune and anxieties to spread their Trojans and worms." To protect against a macro−based exploit, Word users should set macro security level at "Medium," which triggers a warning when a Word document containing one or macros is opened, or "High," to disable macros entirely.
Source: http://www.techweb.com/wire/security/172900939;jsessionid=DI XRDJJ3N5GNGQSNDBCSKH0CJUMEKJVN

31. *October 27, Yahoo News* — **Proposed anti−terror law in France seeks to curtail terrorist activity carried out on the Internet.** One provision in the proposed law extends the period for which cybercafes have to keep records of Internet connection data. One method of cyber−jihad is the "dead letter box" system, wherein someone creates an e−mail account, gives the password to several members of a group and communicates by saving messages in a draft messages folder without sending them. This type of communication often cannot be monitored because government systems for tracking e−mails work only if someone sends an e−mail. Rebecca Givner−Forbes, an intelligence analyst at the Terrorism Research Center states that those behind some Websites promoting terrorism "…often use Japanese and Chinese upload Web pages because they don't ask for an e−mail address or any information from the person uploading a file.” She says the most common method used by terrorist Websites is password−protected online message boards that only members can use. According to Givner−Forbes, "Most recently they have been leveraging the net more and more to circulate terrorist tactical instructions, training manuals, explosives recipes.”
Source: http://news.yahoo.com/s/afp/20051027/tc_afp/internetqaedaatt acks;_ylt=Am7lXspeLmQoK7GhZWLisvr6VbIF;_ylu=X3oDMTBjMHVqMTQ4 BHNlYwN5bnN1YmNhdA−−

32. *October 27, News.com* — **Oracle password system comes under fire.** Experts warn that attackers could easily uncover Oracle database users' passwords because of a weak protection mechanism, putting corporate data at risk of exposure. Joshua Wright of the SANS Institute and Carlos Sid of Royal Holloway College, University of London, say they have found a way to

recover the plain text password from even very strong, well−written Oracle database passwords within minutes. In a presentation given at the SANS Network Security conference in Los Angeles, on Wednesday, October 26, they said that the technique that Oracle uses to store and encrypt user passwords doesn't provide sufficient security. The researchers shared how passwords are encrypted before being stored in Oracle databases. Wright and Cid identified several vulnerabilities, including a weak hashing mechanism and a lack of case preservation (all passwords are converted to uppercase characters before calculating the hash). Wright and Cid wrote "By exploiting these weaknesses, an adversary with limited resources can mount an attack that would reveal the plain text password from the hash for a known user." The researchers said that Oracle users can protect their systems by requiring strong passwords and assigning limited user rights.
Presentation at SANS: http://www.sans.org/rr/special/index.php?id=oracle_pass
Source: http://news.com.com/Oracle+password+system+comes+under+fire/2100−1002_3−5918305.html?tag=nefd.top

33. *October 27, Federal Computer Week* — **Administration to consolidate information technology systems across agencies.** According to Karen Evans, the Office of Management and Budget's administrator for e−government and information technology, the government is looking to consolidate information technology systems and turn them into a "utility" instead of keeping them agency−specific. Rather than restricting IT to individual agencies, IT should be seen as an enterprise, she told members attending the Government Electronics and Information Technology Association (GEIA IT). A recent example is that during the recent hurricane disasters along the Gulf Coast, a number of e−government initiatives were tapped to keep government agencies operational: the Coast Guard and the Transportation Security Administration used the National Finance Center and epayroll.gov to make sure 67,000 customers were paid, and USAServices.gov helped the Federal Emergency Management Agency add call centers and handle over one million calls.
Source: http://fcw.com/article91215−10−27−05−Web

34. *October 27, Government Computer News* — **Executive order bolsters information−sharing among agencies.** On Tuesday, October 25, President Bush issued Executive Order 13356 that restructures information−sharing responsibilities among agencies combating terrorism. The Order grants authority to the Office of the Director of National Intelligence.
Executive Order 13356: http://www.whitehouse.gov/news/releases/2005/10/20051025−5.h tml
Source: http://www.gcn.com/vol1_no1/daily−updates/37432−1.html

35. *October 27, Security Pipeline* — **Microsoft hunts for zombie spammers.** Microsoft is investigating 13 spam operations it believes sent millions of junk mail messages through a single PC that the company purposefully set up as a "zombie," the company said Thursday, October 27. Tim Cranton, the director of Microsoft's Internet Safety division said, "By inserting ourselves in the spammers' path and looking upstream, we have been able to see things we have never been able to see before." The action was coordinated in conjunction with the Federal Trade Commission (FTC) and Consumer Action, a San Francisco−based advocacy group, to identify spammers. Spam operators working in the U.S. could be prosecuted under the federal CAN−SPAM Act. Cranton said, "Hopefully, we'll be able to turn over the results of our investigation for criminal prosecution under CAN−SPAM…We need to take a few more steps, but in the next two to three months, I think we can name these spammers." A new federal

Website can be accessed for consumers to access information on protecting their PCs.
Website: http://onguardonline.gov/index.html
Source: http://www.securitypipeline.com/news/172901034;jsessionid=Y2YXYNET4ZPCEQSNDBCSKH0CJUMEKJVN

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 several buffer overflow vulnerabilities in Skype that may allow a remote attacker to execute arbitrary code. The most critical of these issues can be exploited by sending a specially crafted packet to a vulnerable Skype installation. The are other two vulnerabilities which can be exploited by accessing a specially crafted VCARD or Skype URI. For more information concerning these vulnerabilities can be found in the following US−CERT Vulnerabilities Notes:

VU#905177 − For Skype vulnerable to heap based buffer overflow please see: http://www.kb.cert.org/vuls/id/905177

VU#668193 − For Skype VCARD handling routine contains a buffer overflow please see: http://www.kb.cert.org/vuls/id/668193

VU#930345 − For Skype URI handling routine contains a buffer overflow please see: http://www.kb.cert.org/vuls/id/930345

Skype has released the following Security Bulletins to address these vulnerabilities:

For input on SKYPE−SB/2005−003 please see URL: http://www.skype.com/security/skype−sb−2005−03.html

For input on SKYPE−SB/2005−002 please see URL: http://www.skype.com/security/skype−sb−2005−02.html

US−CERT recommends Skype users to upgrade to the latest fixed version of Skype as soon as possible.

Top Source Port / IP Addresses: Increased reported port activity: 1026 UDP, 1026 UDP, 1029 UDP, 1030 UDP from the following IP blocks, located in China: 221.10.254.31, 222.38.148.21, 218.27.16.180, 221.208.208.8, 221.12.161.99, 220.164.140.226, 202.103.86.66, and 222.241.95.6

ALERT: Trojan Horse Downloaders and Spyware spreading through AIM

US−CERT has received reports of an Instant Messaging worm that targets users of AOL Instant Messenger (AIM). The user receives an unsolicited message within AIM that prompts the user to visit a Website and view a funny picture. The message reads, "so funny hhehe" and is followed by the URL. If the user clicks the URL, an application disguised as a server side PHP script downloads. The application is a variant of the RBOT Trojan Horse, which opens a backdoor on the local machine and connects the user to a BOT Network. The site is hosted in the United States and was up at the time of this alert.

For more information concerning this alert please see URL : http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =324

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 135 (epmap), 139 (netbios−ssn), 25 (smtp), 40000 (−−−), 32789 (−−−), 5274 (−−−) 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

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer