Department of Homeland Security Daily Open Source Infrastructure Report for 26 October 2005

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

Daily Highlights

- The Orlando Sentinel reports Florida's Department of Agriculture and Consumer Services is using gamma rays to help cargo inspectors find drugs, stolen products, illegal immigrants and possibly bombs stashed among the cargo. (See item 11)
- The Food and Drug Administration announces that in response to the emerging threat of pandemic influenza, it has formed a Rapid Response Team to ensure an adequate supply of treatments for stockpiling in the event there is an outbreak in the U.S. (See item 18)

DHS Daily Open Source Infrastructure Report *Fast Jump*

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 25, Associated Press* — **U.S. demonstrates security for Chinese nuclear industry.** The U.S. government is trying to help China's booming nuclear power industry tighten security by conducting demonstrations this week of measures meant to prevent the theft of radioactive material, an American official said Tuesday, October 25. The event is the first of its kind conducted by the U.S. government anywhere in the world, said Linton Brooks, head of the National Nuclear Security Administration, which maintains Washington's nuclear arsenal. It comes as China's nuclear power industry is on the verge of a huge expansion, with plans to build 31 plants by 2020 as Beijing tries to meet soaring power demands. The country has three

plants in operation now. The weeklong demonstrations began Monday, October 24, in Beijing and will involve security systems, technology for tracking radioactive material and export controls, all meant to prevent the theft or diversion of uranium or plutonium, Brooks said. Experts from U.S. nuclear weapons labs prepared the event, which cost $6 million to stage. Participants include Chinese officials and representatives of power plants.
Source: http://www.usatoday.com/news/world/2005−10−25−china−nuclear_x.htm

2. *October 25, Miami Herald* — **Gas supply is fine, but stations suffer outages.** Gas in Florida was plentiful on Tuesday, October 25, but unavailable to motorists wanting to fuel up because most gas stations remained closed due to power outages. Long lines of cars waited at a handful of open stations in Miami−Dade and Broward counties, as gas station owners waited for electricity to be restored. "We're okay on product but we just can't get it out of the ground," said Jim Smith, president of the Florida Petroleum Marketers and Convenient Store Association, which represents 5,600 gas stations throughout Florida. Restoring power on major thorough fares where gas stations are generally located as well as to Port Everglades, South Florida's gas lifeline, were among Florida Power & Light's priorities, said Sarah Williams, a spokesperson with the state's Department of Environmental Protection. “We know that before the storm hit that almost all the gas stations were reporting as having plenty of fuel,” Williams said. “All we have to do now is get the power back on so people can pump it into their cars,” said Williams.
Source: http://www.miami.com/mld/miamiherald/news/breaking_news/12992750.htm?source=rss&channel=miamiherald_breaking_news

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *October 25, Star Ledger (NJ)* — **People evacuated after gas line ruptures.** Police closed Raritan Center Parkway in Paterson, NJ, for an hour Monday, October 24, and evacuated 220 people from nearby businesses after construction crews struck a gas line, causing a leak, police said. Crews from Beach Electrical Co. in Paterson were digging a trench at Fieldcrest Avenue at 10:10 a.m. EDT when they ruptured a two−inch gas line, police said. Police evacuated 180 people from the Wakefern Food Co. on Northfield Avenue and 40 people from the Hillside Warehouse on Fieldcrest Avenue. Officers also closed the road as Elizabethtown Gas Co. worked to fix the leak. The leak was repaired by noon.
Source: http://www.nj.com/news/ledger/middlesex/index.ssf?/base/news−0/113022361065840.xml&coll=1

4. *October 25, WOAI (TX)* — **Worker killed by toxic fumes.** A man was found dead after inhaling toxic fumes and several government agencies have begun investigating the mysterious death. Thirty−three year old Hector Viesca was found dead in a field Saturday night, October 22, in Pleasanton, TX, officials said. Viesca was inspecting oil wells off Corn Road when investigators believe he inhaled hydrogen sulfide. “He checked the tank and what happened was he was supposed to look away,” Pleasanton Fire Marshal Trinidad Vosquez said. “I don't know if he did or didn't.”
Source: http://www.woai.com/news/local/story.aspx?content_id=1484B702−7D45−4103−A505−7AB9A4222253

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *October 25, IT−Observer* — **Rise in spear phishing attacks on businesses.** Spear phishing attacks are the latest technique used by computer hackers to gain access to secure enterprise networks. Unlike common phishing attacks which target millions of users, spear phishing attack is focused on one end−user or an organization at a time, and typically asks for login IDs and passwords. Spear phishing is time−consuming attack which requires computer hackers study the target company and gather as much information as possible on the structure of the company and its personnel from public available sources such as articles, the company Website and telephone inquires. After a successful spear phishing attack, the attacker installs malicious software that gathers and extracts sensitive private and corporate data, often sold to third parties or used for identity theft.
   Source: http://www.ebcvg.com/articles.php?id=944

6. *October 25, Computerworld* — **Security standards combined.** Visa and MasterCard have launched free, self−assessment tools for merchants and providers to test and validate the security of their e−commerce connections. In an effort to combat credit card fraud, both Visa and MasterCard have developed a set of standards for transaction security (called the Payment Card Industry Data Security Standard), a checklist for ensuring systems are up to scratch, and access to a free security assessment tool. Visa head of third−party assurance, Edward Lodens, said the global program to protect cardholder information began in 2001 and since then they have tried to push the information down to the merchant level. "It is essentially three things −− a set of standards called Payment Card Industry Data Security Standard, a foundation framework to validate those standards and tools to validate compliance," Lodens said. "The silver bullet [that will cut down credit card fraud] is the prohibition of storing magnetic stripe authentication data because if there is nothing to steal, nothing can be stolen −− that is the key message," said Lodens.
   Payment Card Industry Data Security Standard:
   http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf
   Source: http://www.computerworld.com.au/index.php/id;701867713;fp;16 ;fpid;0

7. *October 24, Charlotte Business Journal (NC)* — **Data center services provider suffers power outage.** Data center services provider Peak 10 Inc. says its Charlotte, NC, data center suffered an unusual power outage Sunday, October 23, that affected an undisclosed number of customers. The outage was fixed by Monday, October 24, with operations returning to normal, President David Jones says. "Very little data was lost, but the bigger issue is ongoing business and how many transactions were missed on a Sunday night," Jones says. "Determining that

information is part of the recovery process," said Jones. The Website of Charlotte−based online loan exchange LendingTree Inc. was down from about 6:30 p.m. to midnight Sunday because of the outage, spokesperson Rebecca Anderson says. "We had a team of dozens of our technical and operations staff mobilized immediately −− both here at LendingTree and also working with the Peak 10 team at the data center −− and they worked all night" to fix the problem," she says. Jones declines to discuss the specific cause of the problem, but he describes it as a hardware−related issue and not a loss of commercially supplied power. Data center companies provide a range of computer−related services such as Web hosting and data backup for businesses, enabling clients to focus on their core businesses.
Source: http://www.bizjournals.com/charlotte/stories/2005/10/24/dail y8.html?from_rss=1

[Return to top]

Transportation and Border Security Sector

8. *October 25, Associated Press* — **Hurricane Wilma creates problems for airlines.** Upon arrival, Hurricane Wilma created major problems for air travelers on both domestic and international routes. Miami International Airport is the busiest U.S. hub for Latin American travel and the busiest state hub for foreign travel. Yet it was empty on Monday, October 24, and remained that way Tuesday, October 25. At least 2,000 flights −− affecting hundreds of thousands of fliers −− have been cancelled into and out of South Florida's three major airports because of Wilma, and normal service may not resume until the middle of the week. At Fort Lauderdale−Hollywood International Airport, which was closed Monday and didn't immediately announce an exact time when it would fully reopen, Southwest Airlines Co. was hopeful it could resume some sort of schedule into and out of the facility Tuesday afternoon. Southwest did not operate any flights into Fort Lauderdale−Hollywood, Palm Beach International or Fort Myers airports on Monday. Federal Aviation Administration officials said Wilma necessitated the closure of nine Florida airports; others included facilities in Boca Raton, Hollywood−North Perry, Key West, Kissimmee Gateway, Marathon, Fort Myers Page Field, Pompano Beach Airpark and Witham Field in Stuart.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/10 /25/AR2005102500529_pf.html

9. *October 25, 10News (CA)* — **Toys, cookie prompt California airport evacuation.** A suspicious bag forced the evacuation of San Diego International Airport's Commuter Terminal on Tuesday, October 25, an official said. The suspicious items turned out to be toy parts and a cookie, and the terminal was reopened about an hour later. Broadcast reports initially indicated that bomb−making materials had been found in a carry−on bag. However, bomb squad officers determined that the contents of the bag were "not anything of concern," and reopened the terminal, Transportation Security Administration spokesperson Jennifer Peppin said. Screeners saw something that appeared to be suspicious inside a bag at about 7:45 a.m. PDT and called the San Diego Harbor Police, Peppin said. "On the screen it appeared it could have been some sort of IED (improvised explosive device)," Peppin said. As a precaution, officers evacuated the commuter terminal and called a bomb squad, who determined the bag did not contain any explosive material and reopened the terminal, Peppin said. About 170 passengers were evacuated, 10News reported.
Source: http://www.officer.com/article/article.jsp?siteSection=8&id= 26576

10. *October 25, Reuters* — **Bomb threats hit two Los Angeles−area airports.** Two Los Angeles−area airports received bomb threats early on Tuesday, October 25, but searches turned up no explosives. A bomb threat delayed flights at the Long Beach airport and a separate threat at nearby John Wayne Airport was resolved before flights were due to begin, officials said. Long Beach airport police found no bomb following a search and flights were due to resume during the morning. Orange County's John Wayne airport spokesperson Jenny Wedge said it was unclear if the two threats were related.
Source: http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2005−10−25T154027Z_01_YUE548853_RTRUKOC_0_US−SECURITY−USA−THREAT.xml

11. *October 20, Orlando Sentinel (FL)* — **High−tech tool looks into cargo.** New technology utilizing gamma rays is helping cargo inspectors with Florida's Department of Agriculture and Consumer Services find drugs and other contraband, as agents go about their main mission of keeping plant and animal pests and diseases out of the state. The last big catch was $3.4 million of cocaine, which inspectors found inside a truckload of tomatoes last month, using gamma−ray images. The gamma−ray system produces an image of the tractor−trailer's contents in less than two minutes, which authorities say speeds up inspections and allows them to find things they wouldn't have time to search for by hand. The technology −− officially known as the mobile Vehicle And Cargo Inspection System −− also helps to deter criminals. The state operates 22 interdiction stations, on every highway but mainly tracing Florida's north and west borders. They search all commercial trucks hauling plants, produce or meat, in addition to doing random searches of every 20th truck that passes through. Chiefly, the inspectors are supposed to catch pests and diseases that pose a threat to consumers and the state's $62 billion agricultural industry −− but they also look for drugs, stolen products, illegal immigrants or even bombs stashed among the cargo.
Source: http://www.orlandosentinel.com/orl−gamma2005oct20,0,6710624. story

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

12. *October 25, Michigan Ag Connection* — **Two more Michigan deer test positive for encephalitis.** Michigan state officials say they have confirmed two more cases of deer with Eastern equine encephalitis (EEE). That brings the total number of Michigan's confirmed cases in deer to seven. All are from an area of about 25 miles in Kent, southwest Montcalm, and northwest Ionia counties. The disease is more likely to be found in coastal areas and freshwater swamps because it is carried in bird populations and transmitted by mosquitoes.
EEE in Michigan deer map: http://www.michigan.gov/documents/SW_EEE_139356_7.pdf
Source: http://www.michiganagconnection.com/story−state.cfm?Id=627&y r=2005

13. *October 25, Associated Press* — **After eight weeks, Louisiana oysters being harvested.** Louisiana oysters are being harvested again. The beds in the eastern half of the state were tested and retested after Hurricane Katrina to ensure they were clean of chemicals or germs from the water that was pumped out of New Orleans or ran off of other areas. Beds in west Louisiana were closed as a precaution when Hurricane Rita headed in late September. Harvesting began in some areas on Saturday, October 22, and the entire state will probably be open in the next week to 10 days, said Mike Voisin, chairman of the Louisiana Oyster Task Force. Voisin said there were probably 75 or 80 boats out Saturday, about one−fifth or less the usual number for this time of year.
Source: http://abcnews.go.com/US/wireStory?id=1247599

14. *October 24, Stop Soybean Rust News* — **Ten new counties with soybean rust detected in Alabama.** Soybean rust was detected in 10 new counties in Alabama after a survey of roadside kudzu patches and late−season soybean fields was conducted along the eastern edge of the state on October 21 and 22. Ed Sikora, Extension plant pathologist at Auburn University, gave the following report: "Soybean rust was detected in eight of the 16 randomly selected patches surveyed. The kudzu patches were approximately 50−100 meters in length. Rust incidence was relatively low in seven of the eight positive kudzu sites. The counties where rust−infected kudzu was found included: Bullock (2 sites), Barbour, Russell, Chambers, Randolph, Clay, and Marshall. Rust was also detected in three relatively small commercial soybean fields in Cherokee, DeKalb, and Etowah counties in northeast Alabama. Soybean rust has now been found in 26 counties in Alabama. The disease has been observed in 13 commercial soybean fields, 10 soybean sentinel plots, and 12 kudzu patches around the Alabama. Asian soybean rust has now been confirmed in 84 counties in the southeastern U.S. in 2005.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=601

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

15. *October 25, Sun−Sentinel (FL)* — **Residents of 12 cities in Palm Beach County urged to boil water.** A dozen Palm Beach, FL, cities had boil−water orders in effect Monday, October 24, warning residents their drinking water could be contaminated, courtesy of Hurricane Wilma. The upheaval of countless neighborhood trees in Wilma's roughly 100 mph winds ripped up and damaged scores of water mains entwined in their roots. That littered the county with pipe breaks, lowering water pressure and raising the risk of water contamination, county officials said. Pumps needed to push water through lines may also have failed to kick in after power outages, causing weak streams. Water pressure below 20 pounds per square inch can allow contaminants to intrude into lines. More boil−water orders are possible once post−storm water plant assessments are done, Assistant County Administrator Vince Bonvento said. Boca Raton,

FL, which had drinkable tap water, was struggling Monday, October 24, to maintain that. Boynton Beach, FL, was racing to find and plug a slew of water line leaks to keep from going to boiling water, said Peter Mazzella, deputy utilities director. Both of Boynton's plants were running on generator power.
Source: http://www.sun−sentinel.com/news/local/palmbeach/sfl−pwaterewage25oct25,0,3512891.story?coll=sfla−news−palm

[Return to top]

Public Health Sector

16. *October 25, Reuters* — **Officials predict plenty of flu vaccine this year.** At least 70 million doses of influenza vaccine will be available for the U.S. market this year and everybody who wants a shot should be able to get one, health officials said on Monday, October 24. The U.S. Centers for Disease Control and Prevention (CDC) opened flu vaccination to everyone on Monday, October 24. "There is no reason for anyone to delay or go without their annual flu shot," Health and Human Services Secretary Michael Leavitt told reporters in a telephone briefing. Last week the CDC reported that too few Americans are getting their flu shots. An estimated 185 million Americans are considered at high risk of complications including death from influenza. But only about 65 percent of them get the shots. Last year fewer than 60 million people got flu shots. "Seasonal flu kills an average of 36,000 Americans every year. It sends some 200,000 to the hospital," Leavitt said.
Source: http://news.yahoo.com/s/nm/20051025/hl_nm/influenza_dc

17. *October 25, Associated Press* — **Bird flu in China sickens 2,100 geese.** A bird flu outbreak sickened 2,100 geese in eastern China and killed about a quarter of them −− the country's second outbreak reported in a week, a United Nations official said Tuesday, October 25. The Agriculture Ministry confirmed Monday, October 24, that the birds died of the H5N1 virus near Tianchang, a city in Anhui province, said Noureddin Mona, the China representative for the United Nations' Food and Agriculture Organization. The ministry did not say where or when the geese were infected, Mona said. According to Mona, about 45,000 birds have been culled within a three−mile radius of the site. Bird flu has killed at least 61 people and tens of millions of chickens in Asia since surfacing in 2003. Most recently, Russia, Turkey, Britain, and Romania have reported the disease in birds. China has not reported any human infections. Officials began stepping up preventive measures last week after H5N1 killed 2,600 chickens and ducks in a breeding facility in China's northern region of Inner Mongolia.
Source: http://www.usatoday.com/news/world/2005−10−25−geese−bird−flu_x.htm

18. *October 24, Food and Drug Administration* — **Food and Drug Administration announces rapid response team to combat pandemic flu.** In response to the emerging threat of pandemic (Avian) influenza, the Food and Drug Administration (FDA) Monday, October 24, announced the formation of a Rapid Response Team. The team will help ensure an adequate supply of treatments for stockpiling in the event there is an outbreak in the U.S. In partnership with the Department of Health and Human Services, U.S. Centers for Disease Control and Prevention, National Institutes of Health, and industry, the Rapid Response Team will work to ensure every necessary measure is taken to provide an adequate and timely supply of antiviral drugs to treat Avian flu, if it should emerge in the U.S. The Rapid Response Team will address roadblocks to

increased manufacturing of products. The team will support the design and conduct of clinical studies to test new potential treatments for Avian influenza. In the event of a pandemic, such new medications could be made available under Emergency Use Authorization. The team will facilitate the development and availability of safe and effective vaccines that could help protect Americans against a future pandemic. These efforts include measures to help increase vaccine manufacturing capacity and production of currently licensed vaccines using Avian flu strains, and facilitating and evaluating studies that use new technologies.
Source: http://www.fda.gov/bbs/topics/NEWS/2005/NEW01248.html

19. *October 24, Agence France−Presse* — **Volunteers to help fight bird flu in Thailand.** Thailand has assigned 900,000 volunteers to perform house−to−house checks for signs of the deadly avian influenza virus, Health Minister Suchai Charoenratanakul said. The initiative, to be coordinated by more than 9,700 local health offices, comes as Thailand tries to combat bird flu following the country's 13th death from the virus. The volunteer program, which also involves bringing possibly infected subjects to nearby hospitals, is similar to a campaign launched in 2004. Some 957 hospitals across the country have been ordered to ask possibly infected patients whether they lived in affected areas or had any contact with sick or dead chickens before they fell ill, Suchai said in a statement. Last week, Thailand reported its first human fatality from bird flu in a year −− a farmer who slaughtered and then ate a sick chicken. The agriculture ministry has reported 15 outbreaks in four of Thailand's 76 provinces.
Source: http://news.yahoo.com/s/afp/20051024/hl_afp/healthfluthailand_051024205505;_ylt=AruOMtkw89JkEwSyCtW4J0iJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

20. *October 25, Associated Press* — **Emergency preparedness drill in Virginia.** Virginia has set up a four−day emergency−preparedness exercise that includes five states. The drill began on Monday, October 24, with mock reports of widespread illness across western Virginia. The drill included a simulated truck crash that set free a load of possibly diseased prairie dogs. The exercise led by the Virginia Department of Health is testing response efforts and communications among state agencies, 32 hospitals in Virginia, and officials in Virginia, West Virginia, Kentucky, North Carolina, and Tennessee. Participants in Virginia include the state police, FBI, Virginia National Guard, and several state agencies.
Source: http://www.wtkr.com/Global/story.asp?S=4023913&nav=ZolHbyvj

21. *October 25, Portsmouth Herald (NH)* — **Free flu vaccinations available as part of drill.** Portsmouth, NH, city officials and Portsmouth Regional Hospital physicians announced plans Monday, October 24, to test the region’s response to a deadly disease outbreak, should an

outbreak occur. The joint plan to provide 2,000 common flu vaccinations at Portsmouth High School next month as part of a drill comes as worldwide health experts warn of the possibility that the avian flu virus −− which has stricken poultry handlers in Asia −− could mutate into a new strain, posing the threat of a worldwide pandemic. This exercise will provide shots to defend against the "garden−variety" flu virus. The hospital and city officials first planned the exercise after terrorist attacks on September 11, 2001, elevated fears of an outbreak from a bioterrorism attack. The drill will test how agencies would handle traffic flow, communications and other logistics in the case of a real emergency. "In all disasters, the first breakdown is communications −− not being able to contact key town or city officials like the health officer, fire chief, police chief and emergency directors −− which can delay the emergency response to these types of incidents," said Portsmouth Fire Chief Christopher LeClaire.
Source: http://www.seacoastonline.com/news/10252005/news/69630.htm

22. *October 24, Government Technology* — **New York City to deploy security for first responder wireless access.** A Layer 2 secure access solution for enterprise networks, which provides commercially available military−grade security for remote workers' communications over public WiFi hotspots, home wireless networks, and other high−threat remote environments, will be deployed in New York City. The system protects remote users by extending the enterprise network's security perimeter to wired and wireless public networks by separating traffic on the shared network into separate virtual Layer 2 networks. For example, police and fire departments no longer need to set up independent physical networks at an incident site.
Source: http://www.govtech.net/magazine/channel_story.php/97045

[Return to top]

Information Technology and Telecommunications Sector

23. *October 25, IDG News Service* — **German online security program aims to make users aware of software vulnerabilities.** A German program called “Safe in the Net” seeks to make users aware of e−mail viruses, Trojan horses, and other malicious software. The program, launched earlier this year by a German subsidiary of Microsoft, is offering CDs for users of Windows−based computers that contain programs to locate and remove malware and reboot infected machines. The program includes several components, including: an IT security information package with checklists and examples of good IT security practices; support for software developers and students; a security check; an online test certificate; information on how to buy and sell securely on the Internet; and a security barometer, which warns of current viruses, Trojans and other malware. Developers believe that the program could serve as a model for similar programs in other European and North American markets.
Security Initiative: http://www.sicher−im−netz.de.
Source: http://www.infoworld.com/article/05/10/25/HNmsgermansecurity_1.html

24. *October 25, SecurityFocus* — **Multiple vendor anti−virus magic byte detection evasion vulnerability.** Multiple vendor anti−virus software is prone to a detection evasion vulnerability. The problem presents itself in the way various anti−virus software determines the type of file it is scanning. An attacker can exploit this vulnerability to pass malicious files past the anti−virus software. This results in a false sense of security, and ultimately could lead to the

execution of arbitrary code on the user's machine. SecurityFocus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/15189/info

25. *October 25, SecurityFocus* — **Symantec discovery Web accounts default password vulnerability.** Symantec Discovery is prone to a vulnerability regarding the installation password. Remote and local attackers can exploit this issue to gain access to the database without requiring a valid password. This may facilitate further attacks against the database and possibly the underlying system. SecurityFocus reports that Symantec has released patches to address this issue in supported versions.
Symantec Website: http://www.symantec.com/avcenter/security/Content/2005.10.24 .html
Source: http://www.securityfocus.com/bid/15188

26. *October 24, Computer Weekly* — **IT planning vital to meet bird flu pandemic threat.** To prevent a loss of IT functionality in the case of a pandemic, Gartner analyst Dion Wiggins says that it is imperative that companies start planning for a potential outbreak and to look at ways they could use IT to help their businesses continue to function. Companies are encouraged to sign contracts to ship in laptops for staff at short notice, and to provide them with secure virtual private network connections to access office systems. In addition, firms that are heavily reliant on their IT departments should split key IT staff into shifts to maintain consistent coverage. Jim Norton, senior policy adviser at the Institute of Directors, says businesses that invest in broadband and e−commerce technologies are better placed to cope with a pandemic. Business continuity experts said a flu pandemic could cause far more disruption to businesses than the last major flu outbreak in 1968, when businesses were less dependent on a small number of staff with key skills and the smooth running of the transport system for just−in−time deliveries.
Gartner Press Release: http://www.gartner.com/press_releases/asset_138278_11.html
Source: http://www.computerweekly.com/Articles/Article.aspx?liArticl eID=212598&PrinterFriendly=true

27. *October 24, Techworld* — **Oracle's recent security patches may leave serious problems unfixed.** According to Mark Litchfield of Next Generation Security Software (NGSS), who discovered eighteen of the 88 bugs fixed in last week's update from Oracle, the patch could allow attackers to continue taking advantage of some of the bugs. Litchfield says "Having downloaded and given the Oracle October patch a cursory examination, some of the flaws …remain exploitable… the patch is not sufficient." The bugs discovered by NGSS include a buffer overflow vulnerability and 17 PL/SQL injection flaws. Few details have yet been released publicly about most of the flaws.
Oracle Critical Patch Update http://www.oracle.com/technology/deploy/security/pdf/cpuoct2 005.html
Source: http://www.techworld.com/news/index.cfm?newsID=4644&printerf riendly=1

28. *October 24, Networking Pipeline* — **Security group takes first major step against VoIP dangers.** The Voice over IP Security Alliance (VoIPSA) has announced its VoIP Security Threat Taxonomy, which is a classification and description of the types of security threats that affect IP telephony. Alliance secretary and taxonomy project head Jonathan Zar says that the taxonomy is the first step in dealing with VoIP security. By defining the kinds and nature of threats, VoIPSA hopes to give the Internet voice industry a common reference point to deal

systematically with VoIP security issues. The VoIP Security Threat Taxonomy is organized into four broad categories. Two −− denial of service and unlawful signal or traffic modification −− deal with the integrity of the network signal and infrastructure. Signal interception and bypass of refused consent categorize threats specific to VoIP and deal specifically with privacy.
VoIPSA Website: http://www.voipsa.org/
Source: http://www.networkingpipeline.com/showArticle.jhtml?articleI D=172303368

29. *October 22, Secunia* — **RSA authentication agent for Web "redirect" buffer overflow vulnerability.** A vulnerability in RSA Authentication Agent for Web for Internet Information Services has been detected. The vulnerability is caused due to a boundary error in IISWebAgentIF.dll. This can be exploited to cause a stack−based buffer overflow via a GET request with an overly long "url" parameter in the "Redirect" method. The vulnerability has been reported in version 5.2 and 5.3. Other versions may also be affected. According to Secunia, the vendor may have a patch available.
Source: http://secunia.com/advisories/17281/

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 reports a vulnerability in the Snort Back Orifice Parsing Remote Code Execution the exploit is in Snort's Back Orifice pre−processor. A stack based overflow can be triggered with a single UDP packet, allowing an attacker to fully compromise a Snort or Sourcefire installation. X−Force believes this vulnerability to be trivially exploitable, and urges affected users to upgrade immediately. Snort is a widely deployed, open source network intrusion detection system (IDS). Snort and its components are used in other IDS products, notably Sourcefire Intrusion Sensors, and Snort is included with a number of operating system distributions.

Snort preprocessors are modular plugins that extend functionality by operating on packets before the detection engine is run. The Back Orifice preprocessor decodes packets to determine if they contain Back Orifice ping messages. The ping detection code does not adequately limit the amount of data that is read from the packet into a fixed length buffer, thus creating the potential for a buffer overflow. The vulnerable code will process any UDP packet that is not destined to or sourced from the default Back Orifice port (31337/udp). An attacker could exploit this vulnerability by sending a specially crafted UDP packet to a host or network monitored by Snort.

US−CERT is tracking this vulnerability as VU#175500 please review:
http://www.kb.cert.org/vuls/id/175500

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: 221.10.254.31,218. 66.104.208, 222.77.185.242, 221.27.16.180, 61.152.158.126, 221.6.77.72, 202.99.172.160, and 218.66.104.206

US−CERT strongly recommends that all users reference the Federal Emergency Management Agency (FEMA) web site for a list of legitimate charities to donate to their charity of choice. http://www.fema.gov/

Current Port Attacks

Top 10 Target Ports	6346 (gnutella−svc), 1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 12346 (FatBitchtrojan), 135 (epmap), 139 (netbios−ssn), 4495 (−−−), 40000 (−−−), 2234 (directplay) 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

30. *October 25, Quad−City Times (IA)* — **Keeping a camera on parks.** First came banks, then traffic intersections. Now, security cameras are watching over parks in Moline, IL. Moline recently became the first in the area to purchase a camera security system, which uses a combination of technologies to scare off vandals and take pictures that could lead to prosecutions. When someone enters an off−limits area, a voice booms from a loudspeaker. “Stop, it is illegal to spray graffiti here. Your photo has just been taken, and we will use this photo to prosecute you. Leave the area now.” Park officials would not disclose the current location of the camera, which will be rotated among city parks without notice to the public. The city spent $3,600 on the device and has budgeted for a second camera. Mounted in high places, the cameras are contained in a steel case with bullet−proof glass. “You don’t want them being destroyed on you,” said Doug House, director of municipal services.
Source: http://www.qctimes.net/articles/2005/10/25/news/hometowns/doc435db7593c06f315718374.txt

[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