Department of Homeland Security Daily Open Source Infrastructure Report
for 13 October 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

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

Daily Highlights

- U.S. Department of the Treasury reports the start of FloridaFIRST, a coalition formed by a group of Miami financial institutions with the goal of enabling the financial sector in South Florida to handle threats from terrorism and natural disasters. (See item 7)

- The Transportation Security Administration in cooperation with the Truck Renting and Leasing Association has issued a new publication to help truck renting and leasing firms improve security. (See item 10)

- The Baltimore Sun reports Maryland state and local officials plan to investigate why it took more than a day and a half after elevated levels of pollutants were detected in the Westminster water system for a boil order to be issued. (See item 17)

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: <u>Physical</u>: ELEVATED, <u>Cyber</u>: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – http://www.esisac.com]

1. *October 12, Energy Information Administration* — **Energy forecast notes challenges.** Warnings from previous Outlooks about the potential adverse impacts of an active hurricane season on domestic energy supply and prices are unfortunately being reflected in the challenging realities brought about by Hurricanes Katrina and Rita. The impact of the

hurricanes on oil and natural gas production, oil refining, natural gas processing, and pipeline systems have further strained already−tight natural gas and petroleum product markets on the eve of the 2005−2006 heating season (October through March). The combined Short−Term Energy and Winter Fuels Outlook provides a current view of domestic energy supply and prices and provides projections for average household heating expenditures this winter by fuel and by region; baseline forecasts for domestic fuel markets; and projections for international petroleum demand, supply, and price.
Short−Term Energy and Winter Fuels Outlook:
http://www.eia.doe.gov/emeu/steo/pub/oct05.pdf
Source: http://www.eia.doe.gov/steo

2. *October 11, Intelligence Press* — **LNG availability for heating season limited.** With hurricane−related shut−ins damping down nearly seven percent of the Gulf of Mexico's yearly natural gas production, liquefied natural gas (LNG) may be a "supply of last resort" for the coming winter heating season, according to an analysis by Cambridge Energy Research Associates (CERA). However, additional LNG imports may not be available because of global competition, the consulting company reported. "To attract LNG cargoes to U.S. shores, a U.S. buyer must pay a competitive price, including a premium to account for additional shipping distance," said CERA North American gas analyst Robert Ineson. "Increased U.S. demand for additional LNG cargoes comes during a period of limited extra supply availability. Globally, LNG supply has been tight for the past 18 months, leaving numerous ships idle and receiving terminals operating below full capacity," said Ineson. The actual amount of incremental LNG imports will depend on cargo availability and the relative strength of U.S. gas prices as the winter season approaches, Ineson said.
More information from CERA: http://www.cera.com/news/details/1,2318,7648,00.html
Source: http://www.rigzone.com/news/article.asp?a_id=25960

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *October 12, Associated Press* — **Chemical spill at Texas company prompts business evacuation.** Paramedics treated five people after a chemical spill at an electrical products company in east El Paso, TX, on Tuesday, October 11. El Paso Fire Department Lt. Mario Hernandez said the spill occurred when a worker at A.O. Smith apparently knocked over some containers of Xylene. About 50 people from the company and two nearby businesses were evacuated. Hernandez said the workers inhaled fumes from the flammable chemical, which can be used as a solvent. The worker who knocked over five barrels of the chemical, which were originally to be taken to another facility, was taken to a local hospital after having trouble breathing, Hernandez said. The other workers were treated at the scene.
Source: http://thefacts.com/texasstory.lasso?ewcd=4988409b088ec58f

4. *October 12, Associated Press* — **Acid spill in Colorado results in road closure and potential contamination of the Colorado River.** Two containers of acid fell off a flatbed truck traveling on Colorado route 141 early Wednesday, October 12, spilling up to 500 gallons of acid, some of which went into a storm drain that eventually flows into the Colorado River, authorities said. Assistant Fire Chief Greg Martin estimated that 300 gallons went into the storm drain. "We're

trying to find out where we can stop it before it gets into the river," he said. The acid is used in oil and gas drilling, Martin said. He said there was no damage to the road, which was closed for about three hours after the 4 a.m. MDT spill. Crews from the Halliburton Co., which owns the truck and the acid, were on scene to help with the cleanup, Martin said. Also on site were crews from the Grand Junction Fire Department, Colorado State Patrol, and state Department of Transportation.
Source: http://cbs4denver.com/topstories/local_story_285093500.html

5. *October 11, Jackson Channel (MS)* — **Mississippi school evacuated after gas line hit.** Students at Boyd Elementary School in Jackson, MS, returned to class Tuesday morning, October 11, after being evacuated from their classrooms Monday, October 10, when construction crews struck a gas line near the school. The school and 25 nearby homes were evacuated about 10:30 a.m. CDT Monday after the incident occurred. The line was repaired and was back in service Monday night.
Source: http://www.thejacksonchannel.com/news/5083228/detail.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

6. *October 13, Des Moines Register (IA)* — **Counterfeit $100 bills show immunity to detection pens.** The Secret Service has detected a rise in counterfeit $100 bills in Iowa. The bills are resistant to the special pens that are designed to detect counterfeit bills. They have appeared in several grocery stores, although no reports have been made at Wells Fargo locations. Angie Kelso, spokesperson for Wells Fargo, said "They're not seeing it yet. We have an internal communication tool that allows us to notify banks in the area of suspicious activity — counterfeits included."
Source: http://desmoinesregister.com/apps/pbcs.dll/article?AID=/2005 1006/NEWS01/510060393/1002/NEWS01

7. *October 11, U.S. Department of the Treasury* — **Treasury officials attend meeting to address threats to finance sector.** Treasury Under Secretary for Domestic Finance Randal Quarles and Deputy Assistant Secretary for Critical Infrastructure Protection and Compliance Policy Scott Parsons were in Miami, FL, on Thursday, October 13, to join in the unveiling of the FloridaFIRST Regional Coalition. FloridaFIRST is a regional coalition formed by a group of financial institutions based in Miami with the goal of enhancing the resilience of the financial sector in South Florida to handle threats from terrorism and natural disasters. FloridaFIRST is a collective effort to protect the homeland through public and private partnerships. This regional coalition will help officials at all levels of government coordinate with the financial sector in South Florida to share information, promote policies and programs that increase preparedness and to speed the recovery of financial institutions should there be an incident of disruption.

FloridaFIRST is the second regional coalition established in the U.S. ChicagoFIRST was created in 2003 and served as a model for private sector coalitions dedicated to working to protect financial institutions.
ChicagoFIRST: http://www.treasury.gov/press/releases/reports/chicagofirst_handbook.pdf
Source: http://www.treasury.gov/press/releases/js2970.htm

8. *October 11, MSNBC* — **Children's social security numbers often targeted for identity theft.** According to the Federal Trade Commission (FTC), approximately four percent of all identity thefts reported involve children. Linda Foley of the Identity Theft Resource Center says, "I think that's only the tip of the iceberg based on the call volume we are getting here. I would say children of identity theft is closer to about 25 percent of the calls we are receiving." Parents or relatives are often the likely culprits, as they have easy access to their children's social security numbers. The FTC reports that nearly 10 million Americans fall victim to identity theft each year.
Identity Theft Resource Center: http://www.idtheftcenter.org/
Source: http://www.msnbc.msn.com/id/9655565/

[Return to top]

Transportation and Border Security Sector

9. *October 12, Associated Press* — **New antenna installed at Logan.** Federal aviation officials said operations had returned to normal on Wednesday, October 12, at Logan International Airport, following two days of serious delays caused by a faulty radar antenna. The malfunctioning antenna was replaced overnight with one borrowed from the airport in Bangor, ME, Federal Aviation Administration (FAA) spokesperson Arlene Murray said. Over the weekend, air traffic controllers began seeing phantom blips on their radar screens that they knew were not incoming planes. A FAA troubleshooting team from New Jersey arrived Tuesday and identified the radar antenna as the source of the problem. The replacement antenna was brought down from Maine and brought online early Wednesday. "They worked through the night to install the antenna," Murray said Wednesday. Logan began using it at 6:45 a.m. EDT. The problem at Logan prompted the National Air Traffic Controllers Association on Tuesday to publicize a list of operational issues that its leaders say have festered, helping to cause both the radar glitch and recent close calls on Logan runways.
Source: http://www.usatoday.com/travel/news/2005−10−12−logan−delays_x.htm

10. *October 12, Fleet Owner* — **TSA releases truck rental security guide.** The Department of Homeland Security's Transportation Security Administration (TSA) in cooperation with the Truck Renting and Leasing Association (TRALA) has issued a new publication to help truck renting and leasing firms improve security. Entitled "Safeguarding America's Transportation System −− Security Guide for Truck Rental Company Employees," the guide represents just part of a cooperative effort to heighten security awareness within the truck leasing and rental industry. The guide identifies certain behaviors and actions that employees of truck rental companies should be on the look out for during the workday and is expected to augment existing security policies and procedures already in place within the industry. "Security is a top priority for our industry and TRALA will continue to work with government officials and our own security experts in our ongoing commitment to transportation security," said TRALA

president and CEO Peter Vroom.
Security Guide: http://www.trala.org/
Source: http://fleetowner.com/news/TSA_101205/

11. *October 12, Associated Press* — **Governor Perry commits money to border security plan.** Texas Governor Rick Perry on Wednesday, October 12, announced $9.7 million dollars in grants to increase security along the Texas border with Mexico. The funds are part of an initiative to support "Operation Linebacker," which was conceived by the Texas Border Sheriff's Coalition. The governor's Border Security Plan includes six areas: (1) Support local law enforcement and Operation Linebacker. It's envisioned as a means to integrate law enforcement resources along the border to increase public safety and national security between points of entry; (2) Reduce violent crime along the border; (3) Accelerate radio inter−operability, involving communication between multiple agencies; (4) Develop a Bilateral All−Hazards Response Plan; (5) Use the expertise and experience of the National Guard to provide training and participate in response exercises, and (6) Pass legislative reforms, including the expansion of state wiretap authority.
Source: http://www.kristv.com/Global/story.asp?S=3970720

[Return to top]

Postal and Shipping Sector

12. *October 12, BizNewOrleans* — **Mail services return to New Orleans.** The U.S. Postal Service said mail services have been reestablished for every ZIP Code in New Orleans. Postal carriers will make street deliveries where possible and over−the− counter service is available for all others. "We are pleased to be able to reestablish mail services for every ZIP Code in New Orleans," said USPS Louisiana District Manager Tony Ruda. "While delivery remains the objective, the safety of postal employees and customers remains our number one priority." Outgoing mail should be given to postal employees as collection boxes remain sealed.
For the latest information check online at http://www.usps.com or call 1−800−275−8777
Source: http://bizneworleans.com/109+M52816835732.html

[Return to top]

Agriculture Sector

13. *October 12, Agricultural Research Service* — **Cocoa's two most devastating pathogens are close kin.** Scientists with the Agricultural Research Service (ARS) have found that the two most serious fungi infesting the world's cocoa plants are actually "sisters," taxonomically speaking. Using DNA analysis, Cathie Aime, a molecular biologist at ARS' Systematic Botany and Mycology Laboratory, found that the two fungal pathogens causing witches' broom and frosty pod rot are close relatives that really should be classified in the same genus. Witches' broom, caused by the fungus currently known as Crinipellis perniciosa, and frosty pod rot, brought on by Moniliophthora roreri, are the two greatest threats to the world's chocolate supply. Despite widespread fungicide applications, these diseases continue to invade new parts of South and Central America. Despite the pathogens' notoriety, relatively little is known about

the two fungi or their life cycles, making the challenge of their control even more difficult. For the current research, Aime sequenced several genes from the two cocoa pathogens. Almost immediately, she could see that witches' broom and frosty pod were both members of the order Agaricales, the mushroom−forming fungi. Further RNA analysis revealed more detailed evidence pointing to a sister−species relationship between the two. Aime has proposed how to reclassify the two fungi, which, it now appears, share the same ancestor.
Information on Crinipellis perniciosa: http://bp.gsfc.nasa.gov/witchesbroom.html
Information on Moniliophthora roreri: http://www.oardc.ohio−state.edu/cocoa/monilia.htm
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

14. *October 12, Animal and Plant Health Inspection Service* — **Mexico agrees to lift poultry ban on nine states.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service on Wednesday, October 12, announced that Mexico has agreed to lift its ban on poultry, table and hatching eggs and live birds from nine states that had previously had low pathogenicity avian influenza (LPAI). Under the agreement negotiated with officials from Mexico's Secretariat of Agriculture, Livestock, Rural Development, Fisheries and Food, the states of California, Connecticut, Delaware, Maryland, Missouri, New Jersey, North Carolina, Pennsylvania and Texas (with the exception of 11 counties) will now be able to export their products to Mexico. The 11 Texas counties of Gonzalez, Guadalupe, Galdwell, Bastrop, Fayette, La Vaca, De Witt, Karnes, Wilson, Comal and Hays are not covered by the agreement due a 2004 outbreak of high pathogencity avian influenza in Gonzalez County. The United States has agreed to provide Mexico detailed information on its influenza surveillance program and permit them to observe surveillance activities first hand.
Source: http://www.aphis.usda.gov/lpa/news/2005/10/mxlifban_vs.html

15. *October 11, Dow Jones Newswires* — **Permanent bovine spongiform encephalopathy food safety plan seen ready by next year.** The U.S. Department of Agriculture (USDA) will likely have a finished proposal by January 1, 2006, to replace temporary food safety rules that were rushed into effect after a case of mad−cow disease was discovered about two years ago, the department's top food safety official said Tuesday, October 11. Richard Raymond, USDA's food safety undersecretary, said he expects to have the proposal on Secretary of Agriculture Mike Johanns' desk for consideration by the beginning of the year if there are no further delays. One possible delay, he said, could come from USDA's mad−cow surveillance program. USDA continues to test the high−risk population of cattle and has recently begun to test 20,000 healthy−looking cattle. If more cases of mad−cow disease, or bovine spongiform encephalopathy, are found in the apparently healthy cattle, USDA scientists may have to go "back to the start" on the safety rules, Raymond said.
Source: http://www.cattlenetwork.com/content.asp?contentid=11249

[Return to top]

Food Sector

16. *October 12, Food Production Daily* — **Nanotechnology targets new food packaging products.** New nanotechnology products for food packaging are in the development pipeline or, as in the case of anti−microbial films, have already entered the market, according to a report published this month by a European Union−funded research team. "While far reaching visions

such as nanotech food synthesizers or pathogen killing nanobots are not expected to become reality within the next decades, nanotechnology related R&D for food processing, food engineering and food packaging is in the innovation pipeline of the food industry today," the team said. The EU outline report deals with the ethical, legal, and social aspects of nanotechnology as applied to food packaging, energy and medical diagnostics. Along the way it also reveals the developments in food packaging being pioneered by companies, including techniques to improve food safety and supply chain tracking. One big issue in food industry−related R&D is food packaging and food monitoring. In the food−packaging arena, nanomaterials are being developed with enhanced mechanical and thermal properties to ensure better protection of foods from exterior mechanical, thermal, chemical or microbiological effects. "This would endow packaged foods with an additional level of safety and functionality," the researchers stated.

Report: http://www.nanoforum.org/index.php?modul=showmore&folder=999 99&action=longview&scc=news&scid=1786&code=d296c101daa88a51f 6ca8cfc1ac79b50&userid=1707766&wb=155852&

Source: http://www.foodproductiondaily.com/news/ng.asp?n=63147−nanot echnology−food−packaging−research−and−development

[Return to top]

Water Sector

17. *October 12, Baltimore Sun (MD)* — **Reaction to Maryland water alert slow.** Maryland state and local officials pledged on Tuesday, October 11, to investigate why it took more than a day and a half after elevated levels of pollutants were detected in the Westminster, MD, water system for a boil order to be issued −− and why that order was so poorly communicated that few knew about it until the problem had largely resolved itself. Local officials −− who remained confused Tuesday about notification responsibilities −− acknowledged miscommunications and said they will conduct an investigation to find out what went wrong and how to improve their procedures. Although the problem was initially detected about 2 a.m. EDT Sunday, October 9, many local officials were not notified until late Monday afternoon. "We definitely have to address the communication issue," Westminster Mayor Thomas K. Ferguson said. The lagging communications delayed until Monday night a decision to close all public schools in Westminster, left parents scrambling to notify each other, and left residents worrying about the safety of the city's drinking water. "We are disappointed that [Westminster officials] did not know who to contact," said Richard McIntire, a spokesperson for the Maryland Department of the Environment.

Source: http://www.baltimoresun.com/news/local/carroll/bal−md.ca.wat er12oct12,1,6081337.story?coll=bal−local−headlines&ctrack=1& cset=true

18. *October 11, Associated Press* — **Legislative panel begins grappling with water quality proposal.** A state legislative committee on Tuesday, October 11, began grappling with a regulatory proposal that would toughen protection of Iowa's streams and cost nearly $1 billion over 20 years. The proposal before the Administrative Rules Review Committee alters the classification of most Iowa streams to "swimmable, fishable," which dictates the highest protection. That would require upgrades at wastewater treatment plants, factories and other entities that discharge treated water into Iowa's streams. Such point source pollution accounts

for about 20 percent of the pollution in Iowa's rivers and streams, according to the Iowa Department of Natural Resources (DNR). A staff analysis said the cost of those upgrades over a 20−year stretch could range from $790 million to $956 million. Chuck Corell, the DNR's water quality bureau chief said the process would be gradual −− starting with testing next summer and including fieldwork for up to five years before discharge standards change. In some cases, he said, local officials could be given even longer to upgrade their treatment facilities. He suggested in cases where new construction is needed, it could take as long as eight years.
Source: http://www.crgazette.com/2005/10/11/Home/News/waterqualitypr oposals.htm

[Return to top]

Public Health Sector

19. *October 11, Center for Infectious Disease Research and Policy* — **Experts cite differences between H5N1 and ordinary flu.** A recent and extensive review of research on H5N1 avian influenza in humans shows the illness differs from ordinary flu in several ways, besides the most obvious fact that it is far more deadly. Published in the September 29 New England Journal of Medicine by a World Health Organization committee (WHO), the review was written by experts from several countries, including Vietnam, Cambodia, Thailand, the U.S., the United Kingdom, Hong Kong, and Myanmar. The new report says the virus may incubate longer than other human flu viruses before causing symptoms. Incubation periods in ordinary flu range from one to four days. In H5N1 cases, the incubation time has mostly been from two to four days but has stretched to eight days, the WHO report says. Initial symptoms are more likely to include diarrhea in avian flu than in ordinary flu, the report says. The problem can appear up to a week before any respiratory symptoms. That feature suggests that the virus grows in the gastrointestinal tract. The article says the relatively low number of human cases amid widespread infection in birds suggests that the species barrier to human cases of H5N1 is "substantial."
Article: http://content.nejm.org/cgi/content/full/353/13/1374
Source: http://www.cidrap.umn.edu/cidrap/content/influenza/avianflu/news/oct1105flureview.html

20. *October 11, Reuters* — **Indonesia seeks Vietnam advice on fighting bird flu.** Indonesia will study how Vietnam managed to contain an outbreak of bird flu in humans, Jakarta's health minister said on Tuesday, October 11, as the number of positive cases of the deadly virus in the country rose to five. "They have limited resources like us but they were able to properly halt avian influenza," Indonesian Health Minister Siti Fadillah Supari stated after meeting with Vietnamese Health Minister Tran Thi Trung Chien. "We will dissect the case, whether that is because of their eradication measures or something else." Vietnam has recorded 44 deaths from bird flu, the most of any of the four Asian nations where the virus has claimed lives, but there have been no new cases there since July. There have been five confirmed cases in Indonesia since July, comprising three deaths and two people being treated.
Source: http://www.alertnet.org/thenews/newsdesk/JAK266836.htm

21. *October 11, Vietnam News Agency* — **Canada's project to fight new infectious diseases comes to Vietnam.** Steps to carry out a Canada−funded project to fight newly−emerging infectious diseases in Vietnam was the main topic of a two−day seminar held by the

Vietnamese Ministry of Public Health and the Canadian Embassy in Ha Noi. On Monday, October 10, and Tuesday, October 11, domestic and international medical experts gave opinions on a strategic plan for the Canada Asia Regional Emerging Infectious Diseases (CAREID) project. The seminar stressed the tasks that Vietnam should prioritize in the coming time such as defining a mechanism for coordination among donors and mapping out a plan for regional cooperation. The CAREID initiative aims to reduce the threats of infectious diseases in Asia by improving the monitoring and responding capacity related to emerging infectious diseases.

Source: http://www.vnagency.com.vn/newsA.asp?LANGUAGE_ID=2&CATEGORY_ ID=29&NEWS_ID=170060

22. *October 09, Associated Press* — **Japanese encephalitis outbreak claims 15 more lives in India; doctors baffled.** Japanese encephalitis claimed 15 more lives in northern India, as a health official on Sunday, October 9, expressed surprise that the recent outbreak –– which had appeared to be fading –– was spreading again. The outbreak has killed 1,038 people, mostly children, in the impoverished northern states of Uttar Pradesh and Bihar, according to government figures. About 300 deaths have also been reported in neighboring Nepal. The disease is easily preventable by vaccinations, but many medical facilities in the area are underfunded and understaffed. "Cases are now being reported from newer areas," said O. P. Singh, Uttar Pradesh's director general of health services. Reported cases of the mosquito–borne illness had been dropping with the end of the rainy season –– when there's more water for mosquitoes to breed –– and officials had thought it was coming under control. "It is baffling, as new cases are being reported from western part of the state (Uttar Pradesh)," Singh said, adding that a team of specialists has been sent to the area to study the problem.

Source: http://www.khaleejtimes.com/Displayarticle.asp?section=subco ntinent&xfile=data/subcontinent/2005/october/subcontinent_oc tober318.xml

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

23. *October 12, Billings Gazette (WY)* — **Communication interoperability comes first in Wyoming's emergency plans.** More than a month after hurricanes along the Gulf Coast left the nation wondering about governments' ability to respond to a disaster, Wyoming's emergency coordinators say they are well prepared. Communication and planning are keys to effective response, they say. Tom Mahon of the Wyoming Department of Transportation says interoperability is a major concern and that it will be at least two years before the state has met its goals in that area. Mahon was hired by the Wyoming Department of Transportation more than a year ago to manage Wyolink, a statewide program with an initial budget of $54 million to create a network that will allow every state and local agency to communicate on the same radio system. In a crisis, Mahon says, any public safety worker in the state –– emergency

medical technicians, public works road crews, firefighters, police –– will be able to communicate over Wyolink. Federal authorities can use the system, too, if necessary. Mahon said Wyolink is expected to be fully operational statewide by the end of 2007 and will allow for as many as 64,000 users, far more than Wyoming's expected total of about 12,000.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2005/10/12/build/wyoming/25–emergency–plans.inc

24. *October 11, Department of Homeland Security* — **Teachers retrained to help in Louisiana Disaster Recovery Centers.** Teachers, who had been working with Teach For America in Louisiana communities before the hurricanes, started jobs in federal/state Disaster Recovery Centers throughout the state. About 25 teachers have been trained to be managers in existing Disaster Recovery Centers, freeing experienced staff to work in new centers.
Source: http://www.dhs.gov/dhspublic/

[Return to top]

Information Technology and Telecommunications Sector

25. *October 11, Secunia* — **WinRAR format string and buffer overflow vulnerabilities.** Two vulnerabilities in WinRAR can be exploited by malicious people to compromise a user's system. 1) A format string error exists when displaying a diagnostic error message that informs the user of an invalid filename in an UUE/XXE encoded file. This can be exploited to execute arbitrary code when a malicious UUE/XXE file is decoded. 2) A boundary error in UNACEV2.DLL can be exploited to cause a stack–based buffer overflow. This allows arbitrary code execution when a malicious ACE archive containing a file with an overly long file name is extracted. Users should update to version 3.51.
Source: http://secunia.com/secunia_research/2005–53/advisory/

26. *October 11, iDefense* — **SGI IRIX runpriv design error vulnerability.** Local exploitation of a design error vulnerability in the runpriv command included in multiple versions of Silicon Graphics Inc.'s IRIX could allow for arbitrary code execution as the root user. Exploitation requires an attacker to have access to an account which has been granted usage of a binary in the /usr/sysadm/privbin directory. As root must explicitly allow such privileges, the impact of this vulnerability is lessened significantly. Exploitation does not require any knowledge of application internals, making exploitation trivial, even for unskilled attackers.
Vendor patch 7004 for IRIX 6.5.27 and 6.5.28 is available at: http://support.sgi.com/
Source: http://www.idefense.com/application/poi/display?id=312&type=vulnerabilities&flashstatus=true

27. *October 11, Security Focus* — **Linux Kernel multiple memory leak local denial of service vulnerabilities.** Two local denial of service vulnerabilities affects the Linux kernel. These issues are due to a design flaw that creates memory leaks. These vulnerabilities may be exploited by local users to consume excessive kernel resources, likely triggering a kernel crash, denying service to legitimate users. These issues affect Linux kernel versions prior to 2.6.14–rc4. The vendor has released version 2.6.14–rc4 to address these issues.
Source: http://www.securityfocus.com/bid/15076/solution

Internet Alert Dashboard

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 that Microsoft has released updates that address critical vulnerabilities in Windows, Internet Explorer, and Exchange Server. Exploitation of these vulnerabilities may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges or with the privileges of the user. If the user is logged on with administrative privileges, the attacker could take complete control of an affected system. An attacker may also be able to cause a denial of service.

Microsoft Security Bulletins for October 2005 address vulnerabilities in Windows and Internet Explorer. Further information is available in the following US−CERT Vulnerability Notes:

VU#214572 − Microsoft Plug and Play fails to properly validate user supplied data
VU#883460 − Microsoft Collaboration Data Objects buffer overflow
VU#922708 − Microsoft Windows Shell fails to handle shortcut files properly
VU#995220 − Microsoft DirectShow buffer overflow
VU#180868 − Microsoft Distributed Transaction Coordinator vulnerable to buffer overflow via specially crafted network message
VU#950516 − Microsoft COM+ contains a memory management flaw
VU#959049 − Several COM objects cause memory corruption in Microsoft Internet Explorer
VU#680526 − Microsoft Internet Explorer allows non−ActiveX COM objects to be instantiated

Microsoft has provided the updates for these vulnerabilities in the Security Bulletins and on the Microsoft Update site. For more information please visit URL:
http://www.microsoft.com/technet/security/bulletin/ms05−oct. mspx

Top Source Port / IP Addresses: Increased reported port activity: 1028 UDP, 1029 UDP, 1030 UDP, 1434 UPD from the following IP blocks, located in China: 222.77.185.242, 220.164.140.140, 221.10.254.31, 218.27.16.180, 222.77.185.228, 222.241.95.6 , 218.66.104.186, and 220.164.141.140

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), 6881 (bittorrent), 1026 (win−rpc), 5498 (hotline), 445 (microsoft−ds), 40000 (−−−), 135 (epmap), 139 (netbios−ssn), 25 (smtp), 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

28. *October 12, San Francisco Chronicle* — **Mayor wants wider surveillance program.** San Francisco Mayor Gavin Newsom said Tuesday, October 11, that he wanted to expand the surveillance camera program that has been operating on a test basis in the Western Addition to other neighborhoods. Police have reported a drop in violent crime of at least 20 percent in the immediate area of two surveillance cameras installed in late July outside a public housing complex near Eddy and Buchanan streets. The 90−day test period will end this month, and Newsom said he was satisfied with the results.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/c/a/2005/10/12/BABA DIGEST4.DTL

[Return to top]

General Sector

Nothing to report.
[Return to top]

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.

<u>Department of Homeland Security Disclaimer</u>